



2015 International Compendium of  
Data Privacy Laws

**BakerHostetler**

## COUNTRY BY REGION

### Australia

Australia.....	6
----------------	---

### Central Asia

China (People's Republic) .....	37
Hong Kong.....	78
India.....	88
Japan.....	106
South Korea.....	149
Taiwan .....	157

### Central America

Bahamas .....	16
Costa Rica.....	43
Trinidad and Tobago.....	160

### Europe

Austria .....	12
Belgium.....	20
Czech Republic.....	47
Denmark.....	53
Finland.....	58
France .....	63
Germany.....	68
Greece.....	73
Hungary.....	83
Ireland .....	94
Italy.....	99
Luxembourg.....	111
Netherlands .....	125
Spain .....	154
Ukraine .....	164
United Kingdom .....	173

### Middle East

Qatar .....	138
Saudi Arabia .....	143
United Arab Emirates.....	167

### North America

Canada.....	28
Mexico .....	120

### South America

Argentina .....	1
Brazil .....	25
Chile .....	34
Colombia .....	40
Peru.....	130

---

# Table of Contents

Uruguay .....	177
<b>South East Asia</b>	
Indonesia .....	91
Malaysia .....	115
Philippines .....	133
Singapore .....	145

---

# Table of Contents

## COUNTRY INDEX

Argentina.....	1
Australia.....	6
Austria.....	12
Bahamas.....	16
Belgium.....	20
Brazil.....	25
Canada.....	28
Chile.....	34
China (People’s Republic).....	37
Colombia.....	40
Costa Rica.....	43
Czech Republic.....	47
Denmark.....	53
Finland.....	58
France.....	63
Germany.....	68
Greece.....	73
Hong Kong.....	78
Hungary.....	83
India.....	88
Indonesia.....	91
Ireland.....	94
Italy.....	99
Japan.....	106
Luxembourg.....	111
Malaysia.....	115
Mexico.....	120
Netherlands.....	125
Peru.....	130
Philippines.....	133
Qatar.....	138
Saudi Arabia.....	143
Singapore.....	145
South Korea.....	149
Spain.....	154
Taiwan.....	157
Trinidad and Tobago.....	160
Ukraine.....	164
United Arab Emirates.....	167
United Kingdom.....	173
Uruguay.....	177

---

# Welcome

Privacy and data protection issues confront all organizations—whether you handle employee information, credit card data, sensitive financial information, or trade secrets. Securing data is a daunting task that is further complicated by cross-border transfer issues and the differences in privacy laws around the world. These laws are complex and can pose myriad and sometimes conflicting obligations to a multinational enterprise. Our practitioners are experienced at guiding our clients through this maze of global privacy norms.

The BakerHostetler Privacy and Data Protection Team has developed a prompt and practical approach. We have a comprehensive international network of expert service providers who are responsive when our clients require support and guidance through a data security event.

This compendium represents our global experience in this field. While it is not a substitute for legal advice, it is a reference guide that outlines the basic requirements in place when dealing with international data breach so that you can know what immediate steps to take, and what questions you need to ask to minimize your company's exposure.

Our clients call us because we combine our knowledge with the practical experience we have gained through handling over 600 privacy events and working with our international partners around the world.



Theodore J. Kobus III



Gonzalo S. Zeballos

This compendium is provided for informational purposes only. It does not constitute legal advice, and you should not rely on this information in lieu of obtaining such advice. You should consult legal counsel before any decisions or recommendations are made concerning the information contained in this compendium.

---

# Acknowledgements

The preparation of BakerHostetler's International Compendium of International Data Privacy Laws would not have been possible without the invaluable contribution of attorneys and law clerks from BakerHostetler's international data privacy team, whose tireless dedication to research and drafting made this compendium possible:

Alan Pate

Nate Schacht

James Sherer

Maryanne Stanganelli

Elizabeth Stamoulis

Melinda McLellan

## 1. Applicable Law

In Argentina, Personal Data Protection Law No. 25.326, passed in 2000 and restated in Regulatory Decree No. 1558/2001 (“PDPL”), exists to guarantee individuals’ rights of honor and privacy, and to give them access to their personal data. The PDPL applies to all individuals or legal entities, both public and private, who own a database.

<http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm><sup>1</sup>

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** National Commission for the Protection of Personal Data, or Direccion Nacional de Proteccion de Datos Personales (“Commission”). Information on the Commission is available at: <http://www.jus.gov.ar/datos-personales.aspx>.
- 2.2 **Registration.** Public and private databases must register with the Commission before they may process data unless otherwise exempted. Exemptions include private databases intended for exclusively personal use.
- 2.3 The registration with the Commission should include at least the:
  - name and address of the owner or controller of the database;
  - characteristics and purpose of the database;
  - nature of the personal data in each database;
  - method of collection and updating of data;
  - destination of the data and persons or legal entities to whom such data may be transmitted;
  - manner in which the recorded information can be interrelated;
  - details regarding data security, including the means used to ensure data security;
  - data preservation term; and
  - procedure and conditions under which persons may have access to their data and procedure to rectify or update such data.

## 3. Protected Personal Data

- 3.1 **Personal data** is any information relating to ascertained or ascertainable individuals or legal entities. However, the PDPL does not cover data from opinion polls, statistical research under Law 17,622 (governing the National Institute of Statistics and Censuses), market research, and medical or scientific investigations, so long as the information cannot be linked to an identified or identifiable individual or legal entity.

---

<sup>1</sup> An unofficial English translation of the law has been made publicly available online by [protecciondedatos.com](http://protecciondedatos.com). It is available at [www.protecciondedatos.com.ar/law25326.htm](http://www.protecciondedatos.com.ar/law25326.htm).



- 3.2 **Sensitive personal data** is defined as information about a data subject's racial or ethnic origin, political opinions, moral/religious/philosophical beliefs, union membership, health, or sexual habits or behavior.

#### 4. Data Collection and Processing

- 4.1 The collection and processing of personal data is unlawful when the data owner has not given his or her express consent, which must be freely given in writing, or by equal means, depending on the circumstances. The consent must be informed by information provided in advance, as summarized in Section 4.3.

- 4.2 Consent is not necessary when the data:

- are secured from a source of unrestricted public access;
- are collected for the performance of the duties inherent in the powers of the State;
- consists of lists limited to name, national identity card number, taxing or social security identification, occupation, date of birth, domicile and telephone number;
- arise from a contractual scientific or professional relationship with the data owner, and are necessary for its development or fulfillment; or
- refer to transactions performed by financial entities, and arise from information received from customers under Section 39 of Law number 21,526.

- 4.3 When personal data is requested, data owners must first expressly and clearly inform the data subject:

- the purpose for which the data shall be processed, and to whom the data will be received or may be received;
- the existence of the relevant database, whether electronic or otherwise, and details regarding the person responsible for the database;
- whether answers to the information requested are compulsory or not;
- the consequences of providing the data, or refusing to provide the data, or providing inaccurate data; and
- regarding the availability of access, rectification and suppression rights.

- 4.4 PDPL requires that personal data for collection and processing must be:

- accurate, appropriate, pertinent and not excessive in relation to the scope and purpose for which it was secured;
- not collected using unfair or fraudulent means;
- updated if necessary, and, when becoming aware that data is wholly or partially inaccurate or incomplete, the individual responsible for the database must see it suppressed and replaced, or—if relevant, completed;
- stored such that a data owner can exercise his or her right of access; and
- destroyed once it ceases to be necessary or relevant to the purposes for which it was collected.

- 4.5 Special Considerations Regarding Sensitive Data

No person can be compelled to provide sensitive data. The PDPL prohibits the establishment of databases that directly or indirectly reveal sensitive data, except in some circumstances. However, sensitive data can be collected and processed for:

- general interest reasons as defined by law; and
- statistical and scientific purposes, provided the data subjects cannot be identified.

4.6 Data regarding criminal convictions or misdemeanors can only be processed by the relevant authorities.

## **5. Data Transfer**

5.1 Personal data may only be transferred with the data subject's consent after the data subject is informed of the purpose of the transfer and the identity of the transferee unless consent is provided by law, the transfer is made by a government agency under legal authority, the data subject is not identifiable, or other exceptions.

5.2 Any database containing sensitive data must encrypt the information when it is transported or transferred to a third party.

5.3 International Data Transfer

Generally, the transfer of any type of personal information to countries or international or supranational entities that do not provide adequate levels of protection (adequate protection levels may arise from contractual clauses or other means) is prohibited. This prohibition does not apply in the following circumstances:

- when the subject of the data has consented to the transfer;
- international judicial cooperation;
- exchange of medical information for medical treatment (or in the case of an epidemiological survey provided that information is dissociated so that the person to whom the information refers is unidentifiable);
- stock exchange or banking transfers, to the extent thereof, and in pursuance of the applicable laws;
- when the transfer is arranged within the framework of international treaties to which the Argentine Republic is a signatory; or
- when the transfer is made for international cooperation purposes between intelligence agencies in the fight against organized crime, terrorism, or drug-trafficking.

## **6. Data Security**

The PDPL itself does not specify the type of security measures to adopt and implement for the safeguarding of personal data; however, it does indicate that the user of data files must take such technical and organizational measures as are necessary to guarantee the security, integrity, and confidentiality of personal data, in order to avoid their alteration, loss, unauthorized consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information.

However, the Commission laid out mandatory security measures in Directive 11/2006 ([http://www.ius.gob.ar/media/33445/disp\\_2006\\_11.pdf](http://www.ius.gob.ar/media/33445/disp_2006_11.pdf)). It provides for basic, intermediate and critical levels of security, depending on factors such as the nature of the data and the risks involved.

## **7. Breach Notification**

The PDPL and its implementing decree do not contain any provisions with regard to data breach notification. However, security incidents must be recorded as part of security measures required under Directive 11/2006.

## **8. Other Considerations**

### **8.1 Right of Habeas Data**

Habeas data is a right incorporated into Argentina's data protection law that allows an individual to have access to any data about them contained in a database. The law provides a comprehensive process to exercise this right, but, in summary, every person has the right to take legal action to access the data about them contained in public or private databases. They may also request that the data be removed, updated, rectified—or where applicable, suppressed—if it can be proven to be incorrect or confidential.

### **8.2 The PDPL contains special rules for databases involved in providing credit information services, advertising, and opinion polls.**

## **9. Enforcement & Penalties**

The Commission has the authority to impose the following sanctions:

### **9.1 Administrative Sanctions**

- warning;
- suspension;
- a fine of between 1,000 pesos and 100,000 pesos; or
- closure or cancellation of the file, register or database.

### **9.2 Criminal Sanctions**

The PDPL adds the following criminal sanctions to the Argentine Criminal Code:

- a penalty of imprisonment for the term of one month to two years shall apply to anyone who knowingly inserts or has false information inserted in a personal data file;
- the penalty shall be from six months to three years to anyone who knowingly disseminates to a third party false information contained in a personal data file;
- the punishment scale shall be increased by one-half of the minimum and the maximum penalties when a person is harmed as the result of the above-mentioned action; and
- a penalty of six months to three years of imprisonment shall be applied to anyone who:
  - knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into a personal database;
  - discloses to third parties information registered in a personal database that should be kept secret by provision of law; or
  - where the offender is a public officer, an accessory penalty consisting in a special disqualification for a term of one to four years.

## 1. Applicable Law

In Australia, data privacy is governed at the federal level by the Privacy Act of 1988 (the “Act”). The Act applied to Commonwealth, Australian Capital Territory government entities, and credit reporting organizations until December 2001, after which the Privacy Amendment (Private Sector) Act 2000 added private sector organizations and businesses that earn more than \$3 million annually.

<http://www.comlaw.gov.au/Details/C2012C00903>

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 containing significant amendments to the Act came into effect on March 12, 2014.

<http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform>

Although this summary focuses on federal law in Australia, it is important to note that there are state- and territory-level laws and authorities regarding data protection as well. The Office of the Privacy Commissioner provides information and links on the various state and territory privacy and data protection-related laws and, where applicable, authorities for each, at <http://www.privacy.gov.au/law/states/act>. The privacy commissioners for certain Australian states and territories have their own websites, as follows:

- New South Wales  
<http://www.ipc.nsw.gov.au>
- Victoria  
[www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)
- Queensland  
[www.oic.qld.gov.au](http://www.oic.qld.gov.au)
- Northern Territory  
[www.privacy.nt.gov.au](http://www.privacy.nt.gov.au)

## 2. Data Protection Authority and Registration Requirements

2.1 **Federal Authority.** The Office of the Privacy Commissioner. Their website is available at: <http://www.oaic.gov.au/>.

2.2 **Federal Registration.** Australian federal law does not require data collectors to register with the Office of the Privacy Commissioner.

## 3. Protected Personal Data

3.1 **Personal information** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

3.2 **Sensitive information** means personal information or an opinion about an individual's

- race 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 preferences or practices;
- criminal record; or
- health information about an individual or genetic information about an individual that is not otherwise considered health information.

#### **4. Data Collection and Processing**

As relates to the private sector, the Privacy Act 1988 contains ten National Privacy Principles in Schedule 3. Many of these relate to data collection and processing.

- 4.1 An organization covered by the Act is prohibited from collecting personal information unless that information is necessary for one or more of its functions or activities.
- 4.2 At or before the time (or, if that is not practicable, as soon as practicable after) an organization collects information about an individual, the organization must take reasonable steps to ensure that that individual is aware of certain information:
- the identity of the organization and how to contact it;
  - the fact that he or she is able to gain access to the information;
  - the purposes for which the information is collected;
  - the organizations to which the organization usually discloses information of that kind;
  - any law that requires the particular information to be collected; and
  - the main consequences (if any) for the individual if all or part of the information is not provided.

An organization must generally collect personal information about an individual only from that individual. If not reasonable or practical to do so, an organization may collect personal information about an individual from someone else, but it must take reasonable steps to ensure that the individual is or has been made aware of the above information, unless would pose a serious threat to the life or health of any individual.

- 4.3 An organization cannot use or disclose personal information about an individual for a purpose other than the primary purpose of collection unless it obtains the individual's consent.
- 4.4 Consent is not necessary where:
- the secondary purpose is related to the primary purpose and the individual would reasonably expect the information to be used or disclosed for the secondary purpose;

- the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing where:
  - it is impracticable for the organization to seek the individual's consent before that particular use;
  - the organization will not charge the individual opting out of direct marketing communications;
  - the individual has not made a request to the organization not to receive direct marketing communications;
  - in each direct marketing communication with the individual, the organization draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
  - each written direct marketing communication by the organization with the individual (up to and including the communication that involves the use) sets out the organization's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organization can be directly contacted electronically;
- the information is health information and its use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety and the following conditions apply:
  - it is impracticable for the organization to seek the individual's consent before the use or disclosure;
  - the use and disclosure is conducted in accordance with guidelines approved by the Office of the Privacy Commissioner; and
  - in the case of disclosure—the organization reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information;
- the organization reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, or safety; or a serious threat to public health or public safety;
- if the information is genetic information and the organization has obtained the genetic information in the course of providing a health service to the individuals, there are even further exceptions that can apply;
- the organization has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;
- the use or disclosure is required or authorized by law; or
- the organization reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
  - the prevention, detection, investigation, prosecution or punishment of criminal offenses, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

- the enforcement of laws relating to the confiscation of the proceeds of crime;
- the protection of the public revenue;
- the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; and/or
- the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

#### 4.5 Special Considerations Regarding Sensitive Information

An organization governed by the Act cannot collect sensitive information about an individual unless:

- the individual has consented;
- the collection is required by law;
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns is: (i) physically or legally incapable of giving consent to the collection or (ii) physically cannot communicate consent to the collection;
- the information is collected in the course of the activities of a non-profit organization and:
  - the information relates solely to the members of the organization or to individuals who have regular contact with it in connection with its activities; and
  - at or before the time of collecting the information, the organization undertakes to the individual whom the information concerns that the organization will not disclose the information without the individual's consent; or the collection is necessary for the establishment, exercise or defense of a legal or equitable claim.

#### 4.6 Further Consideration for Health Information

Beyond those mentioned above, the National Privacy Principles provide further, detailed exceptions related to health information in certain situations.

### 5. Data Transfer

5.1 A record-keeper in possession of personal information is prohibited from disclosing that information unless the:

- individual concerned is reasonably likely to have been aware that information of that kind is usually passed to that person, body or agency;
- individual concerned has consented to the disclosure;
- record-keeper reasonably believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
- disclosure is required or authorized by law; or
- disclosure is reasonably necessary for the enforcement of criminal law or of a law imposing a pecuniary penalty, or for the protection of the public review.



- 5.2 Third parties cannot use or disclose the information they have been given for a purpose other than that for which they were given the information.
- 5.3 International Data Transfer. An organization is prohibited from transferring personal information to another organization in another country unless:
- the organization reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles;
  - the individual consents to the transfer;
  - the transfer is necessary for the performance of a contract between the individual and the organization, or for the implementation of pre-contractual measures taken in response to the individual's request;
  - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organization and a third party;
  - all of the following apply:
    - the transfer is for the benefit of the individual;
    - it is impracticable to obtain the consent of the individual to that transfer; and
    - if it were practicable to obtain such consent, the individual would be likely to give it; or
  - the organization has taken reasonable steps to ensure that the information that it has transferred will not be held, used, or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

## **6. Data Security**

An organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure. An organization must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information originally could be used or disclosed under the Act.

## **7. Breach Notification**

Australian organizations are not required under the Act to notify anyone of a breach in their data security. Instead, the Office of the Privacy Commissioner has issued voluntary guidelines for when and how to report a breach. Furthermore, the Office of the Privacy Commissioner states that having in place a breach notification system may be considered part of the "reasonable steps" required for data security.

## **8. Enforcement & Penalties**

- 8.1 Enforcement under the Act is accomplished by the response to complaints by the Office of the Privacy Commissioner. After investigating a complaint, the Office of the Privacy Commissioner is empowered to make a determination containing any of the following declarations:

- an organization has not complied with the Act;
  - that an organization should undertake a course of conduct to redress any loss or damage suffered by the complainant; or
  - that the complainant is entitled to compensation for any loss resulting from the subject of the complaint.
- 8.2 A determination by the Office of the Privacy Commissioner can be enforced by commencing proceedings in the Federal Court or the Federal Magistrate Court.
- 8.3 While most complaints are resolved without a formal determination, the Office of the Privacy Commissioner has issued nine determinations since the Act was passed in 1989.
- 8.4 There are penalties for refusing or failing to attend before the Commission, or to be sworn or make an affirmation, of up to AUD 2,000 or 12 months imprisonment, or both. This does not apply if there is a reasonable excuse. There are penalties of up to AUD 2,000 or 12 months imprisonment, or both, for making a knowingly false or misleading statement that is material. The same penalty applies for refusal or failure to assist an investigation (or to answer a question or produce a document or record), except that for corporations the penalty is AUD 10,000.

## 1. Applicable Law

In Austria, data privacy is governed by the Austrian Data Protection Act 2000 (“DSG”), which implements the EU Data Protection Directive 95/46/EC and applies to the use of personal data in Austria and outside Austria in some cases. The DSG does not apply to data that is processed in Austria where the controller is elsewhere in the EU or where data is only transmitted through Austrian territory.

There are some Austrian laws in other subject areas that also relate to data protection. For example, the Labor Relations Act, the Banking Act, the Trade Regulations Act, and the Telecommunications Act. The latter includes provisions on the use of cookies and the processing of traffic data specifically for the telecommunications industry.

<http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597>

<http://www.dsb.gv.at/DocView.axd?CobId=41936> (Unofficial English Translation)

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Austrian Data Protection Authority, or Datenschutzbehörde (“DSB”).

2.2 **Registration.** The DSB operates a register of data controllers and their data applications. The data controller must file a notification before commencing a data application. The DSG provides a list of notification requirements that include, for example:

- the name and address of the controller and, where applicable, of her representative;
- the purpose of the data application and the legal basis for the same;
- categories of data subjects and of personal data processed;
- categories affected by the transfer of data and categories of recipients, including possible recipient states abroad;
- file of the permit number to the extent one is required by the DSB; and
- a description of security measures.

There are some data applications that are not subject to notification, such as for exclusively personal use, use of published data, and more.

## 3. Protected Personal Data

3.1 **Personal data** is information about an identified or identifiable person. “Persons” include natural persons and legal entities.

3.2 **Sensitive data** is information about a natural person’s racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, health, or sex life.

- 3.3 **Indirect data** is personal data for which the identity of the subject can be found only through illegal means.

#### 4. Data Collection and Processing

- 4.1 The data controller must generally inform the data subject of the purpose of the processing and the name and address of the controller. The data subject must be informed of other information if good faith dictates it, such as whether the subject has the right to object to the processing or transmission of data.

- 4.2 Personal data may be processed if:

- an explicit authorization or obligation to use the data exists;
- the data subject has given his revocable consent;
- the vital interest of the data subject requires the use; or
- overriding legitimate interests pursued by the controller or by a third party require the use of the data.
  - in particular this occurs if the use of the data is required to protect the vital interests of a third party, is necessary for the fulfilment of a contract between the controller and data subject, concerns the exercise of a public office by the data subject, and more.

- 4.3 Sensitive personal data may only be processed, in the absence of unambiguous revocable consent from the data subject, if:

- the data subject has obviously made the data public himself;
- the data are used only in indirectly personal form;
- the obligation or authorization to use the data is stipulated by laws, insofar as these serve an important public interest;
- the use is made by a controller of the public sector in fulfillment of his obligation to give inter-authority assistance;
- the data solely concerns the exercise of a public office by the data subject;
- the data subject has unambiguously given his consent, which can be revoked at any time;
- the processing or transmission is in the vital interest of the data subject and the data subject's timely consent cannot be obtained;
- the use is in the vital interest of a third party;
- the use is necessary for establishment, exercise or defense of legal claims of the controller before a public authority and the data has been legitimately collected;
- the data are used for private purposes or purposes relating to certain scientific, statistical, and public purposes, or for interviewing, or in the case of a catastrophe in accordance with the other provisions of the DSG;
- the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations and, is legitimate according to specific legal provisions;
- the data are required for the purposes of preventative medicine, medical diagnosis, the provision of health care or treatment or the management of

- health-care services, and the use of the data is performed by medical personnel or other persons subject to an equivalent duty of secrecy; or
- a political, philosophical, religious, or trade union non-profit organization processes the data in the course of their legitimate activities, in a manner that reveals the data of members who display an interest in the aim of the organization on a regular basis.

## 5. Data Transfer

- 5.1 Data transfer, including when the controller allows a different party to process the data, is only allowed if the recipient can show that it can ensure legal and secure processing. Data subjects do not need to be informed of the transfer where the processing is required by law, the subject cannot be reached, or the infringement on the subject's rights is very unlikely, and the costs of informing all data subjects are excessively high. The controller has no duty to inform the data subject if the controller would not be required to notify the DSB of the transfer.
- 5.2 International Data Transfer. The international transfer of data requires prior authorization from the DSB, unless:
- the data subject has given unambiguous consent;
  - the transmission is to a recipient within a signatory state of the European Economic Area;
  - the transmission is to a country that has been declared in an Austrian ordinance to have an adequate level of protection;
  - the data has been legitimately published in Austria;
  - the data are only indirectly personal to the recipient;
  - the transmission is authorized by regulations that are equivalent to Austrian statutes;
  - the data is for private or journalistic purposes;
  - 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 international transmission of data;
  - the transmission is necessary for the establishment, exercise or defense of legal claims before a foreign authority and the data were collected legitimately;
  - the transmission is expressly named in a standard or model ordinance;
  - the data is being exchanged with Austrian governmental missions and offices in foreign countries; or
  - the transmissions are made from a data application that is exempted from notification under the statute.

There is another exception, where the transmission is necessary to safeguard an important public interest or the vital interest of a person and timely authorization cannot be obtained. However, in that case the DSB must be notified immediately.

In addition, countries with an adequate level of protection include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be

permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

The binding corporate rules framework and EU model contractual clauses are relevant to DSB authorization. See <http://www.dsb.gv.at/site/6208/default.aspx>.

## **6. Data Security**

Although the type and extent of security measures varies with the type of data processed and other factors, all security measures must ensure: (i) protection against accidental or illegal destruction of data, (ii) proper processing, and (iii) that the data is only accessible to authorized persons. These include a number of measures, for example, regulation of access to the premises, instruction to every operative regarding his or her duties, and maintenance of logs with information on processing.

## **7. Breach Notification**

If the data controller becomes aware of a breach and that data has been systematically and seriously misused and the data subjects may suffer damages, the controller must immediately notify the subjects in an appropriate manner. However, if notification would require disproportional effort and cost compared to what would likely be minor damage to the data subjects, there is no notification obligation.

## **8. Enforcement & Penalties**

A data subject may file a complaint with the DSB. A data subject may file a complaint in civil court or apply for an injunction where the data subject's right to data protection or to correction or deletion is infringed upon, or for damages where the infringement was caused by negligent conduct and resulted in financial loss.

The willful infringement of data protection with the intention of unjustified enrichment or to harm another person carries a criminal sanction of up to one year in prison. Other more minor violations of the DSG can result in administrative penalties of up to €25,000.

## 1. Applicable Law

The [Data Protection Act 2003](#) (the “Act”) governs data processing and the handling of personal data. The Act went into effect on April 2, 2007, with a one-year grace period to allow organizations to comply, as part of an effort to protect financial sector data. The Act applies to processors with an establishment in the Bahamas or by a processor without an establishment in the Bahamas if equipment in the Bahamas is used to process the data, though not if the data merely is transmitted through the Bahamas.

<http://www.lexbahamas.com/Data%20Protection%202003.pdf>

## 2. Data Protection Authority and Registration Requirements

The Office of Data Protection Commissioner (“Commissioner”) is charged with creating codes of practice with regard to the protection of personal data, investigating violations of the act, and prosecuting offenses in the magistrate court.

[http://www.bahamas.gov.bs/wps/portal/public!/ut/p/b1/04\\_Sj9CPykssy0xPLMnMz0vMAfGjzOKNDdx9HR1NLHz9jUIsDTwNnQ3NvENNDXyMjIAKIoEKDHAARwNC-sP1o\\_ArMYAqwGOFn0d-bqp-QW6EQZaJoyIAImmmzA!!/dl4/d5/L2dBIS9nQSEh/](http://www.bahamas.gov.bs/wps/portal/public!/ut/p/b1/04_Sj9CPykssy0xPLMnMz0vMAfGjzOKNDdx9HR1NLHz9jUIsDTwNnQ3NvENNDXyMjIAKIoEKDHAARwNC-sP1o_ArMYAqwGOFn0d-bqp-QW6EQZaJoyIAImmmzA!!/dl4/d5/L2dBIS9nQSEh/)

The Commissioner has issued a number of guidance manuals, including A Guide for Data Controllers (“Guidelines”) and guidance for managing a data security breach (“Breach Guidance”), provided below.

- [Managing a Data Security Breach](#)
- [A Guide for Data Controllers](#)

## 3. Protected Personal Data

- 3.1 **Personal data** is data relating to a living individual who is or can be identified from either the data or the data in conjunction with other information in the possession of the data controller. The Guidelines add “or is likely to come into” the possession of the data controller to this definition.
- 3.2 **Sensitive personal data** is data relating to a person’s racial origin, political opinions or religious or other beliefs, physical or mental health, sexual life, criminal convictions or alleged offenses, and trade union membership.

## 4. Data Collection and Processing

The text of the Act provides basic principles, the Guidelines, which indicate they are not authoritative, provide specific recommendations for carrying out the general principles.

- 4.1 Under the text of the Act, data must be collected and processed by means which are lawful and fair in the circumstances of the case. Data must also be:
- kept accurate and up to date;
  - kept for only one or more specified and lawful purposes;
  - not used or disclosed in any manner incompatible with the lawful purpose for which it was collected;
  - adequate and relevant in relation to the purpose for which it was collected; and
  - not retained longer than necessary for the purpose it was collected.
- 4.2 The Guidelines provide certain notice requirements for data collection and procession. Under the Guidelines, to fairly obtain the data, at the time of data collection, the data collector must make the data subject aware of:
- the data controller's identity;
  - the purpose of collecting the data;
  - the people and categories of people to whom the data may be disclosed; and
  - any other information necessary to make the data processing fair.
- 4.3 Under the Guidelines, data may only be processed if the data subject has given consent, or the processing is necessary:
- to prevent injury or other damage to the health of a data subject;
  - to prevent injury to property of the data subject;
  - to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damages;
  - for the administration of justice;
  - for the performance of a function conferred on a person by or under an enactment;
  - for the performance of a function of the Minister or Minister of National Security;
  - for the performance of any other function of a public nature performed in the public interest by a person; or
  - for the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.
- 4.4 The Guidelines set forth additional requirements before a party can process sensitive personal data. The data subject must either give explicit consent to the processing, or the processing must fit one of the following circumstances:



- for the purpose of exercising or performing any right or obligation that is conferred or imposed by law on the data controller in connection with employment;
- to prevent injury to health or serious loss to property;
- to protect the vital interests of the data subject or another where consent cannot reasonably be obtained;
- it is carried out by a not for profit organization in respect of its members or other associated parties;
- the information being processed has already been made public as a result of deliberate steps taken by the data subject;
- for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights;
- for medical purposes; or
- it is carried out by political parties or candidates for election in the context of an election.

## 5. Data Transfer

- 5.1 Any disclosure or use of data must be necessary for—or compatible with—the purposes for which the data was collected. Restrictions on the disclosure of personal data do not apply if the disclosure is:
- in the opinion of the Minister or the Minister of national Security required for the purpose of safeguarding the security of The Bahamas;
  - required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the government, statutory corporation, public body, or local authority;
  - required in the interests of protecting the international relations of The Bahamas;
  - required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
  - required by or under any enactment or by a rule of law or order of a court;
  - required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness;
  - made to the data subject concerned or to a person acting on his behalf; or
  - made at the request or with the consent of the data subject or a person acting on his behalf.
- 5.2 Data controllers should have a contract with any third-party processors imposing the same security obligations that apply to the processor.
- 5.3 International Data Transfer. The Commissioner may prohibit the transfer of personal data outside the Bahamas. In doing so, the Commissioner will consider whether the transfer would be likely to cause damage or distress to any person and the desirability of facilitating international transfers of data. Any prohibition does not apply where the transfer is required for the Bahamas to comply with an international obligation.

## **6. Data Security**

The Act requires that “appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.” Accordingly, the Breach Guidance suggests a policy to manage a data security breach “may be prudent.”

## **7. Breach Notification**

- 7.1 There is currently no requirement. While not affirmatively required under the law itself, the Breach Guidance provides that notification regarding a data breach can be an important element in a data breach strategy. The Breach Guidance provides questions for consideration regarding whether to notify, and provides that where a large number of people are affected or there are very serious consequences, the Commissioner should be notified.
- 7.2 The Breach Guidance further notes that if a decision to notify is made, such notification to individuals should have a clear purpose, use the most effective and secure medium, and should at least include a description of how and when the breach occurred and what data was involved, as well as details of the response to the risks posed by the breach. Giving specific and clear advice on how to contact the data controller for more information and steps individuals can take to protect themselves are also mentioned.
- 7.3 Notification to the Commissioner should include details of the security measures in place, such as encryption, and, where appropriate, details of the security procedures in place at the time of breach. The Breach Guidance further suggests consideration of notification to third parties such as the police, insurers, professional bodies, and bank or credit card companies.

## **8. Other Considerations**

Except in certain situations, individuals have the right to access their information.

## **9. Enforcement & Penalties**

Anyone guilty of offending the Act faces fines on summary conviction of up to \$2,000 or on conviction on information up to \$100,000. Further, a data controller may be ordered to delete all or part of the database.

## 1. Applicable Law

Belgium implemented the EU Data Protection Directive by enacting the *Law on the protection of privacy in relation to the processing of personal data* (“DPL”). The DPL was passed on December 8, 1992. The DPL and took effect on September 1, 2001, and applies to activities of a data controller permanently established in Belgium or to which Belgian law applies or to controllers who are not established in Belgium if the means of processing is located in Belgium. The DPL does not apply, however, to data that is only transmitted through Belgium.

<http://www.privacycommission.be/sites/privacycommission/files/documents/wet-8121992-be.pdf>

[http://www.privacycommission.be/sites/privacycommission/files/documents/CONS\\_loi\\_vie\\_priv\\_e\\_08\\_12\\_1992.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/CONS_loi_vie_priv_e_08_12_1992.pdf) (in French)

[http://www.privacycommission.be/sites/privacycommission/files/documents/CONS\\_wet\\_privacy\\_08\\_12\\_1992.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/CONS_wet_privacy_08_12_1992.pdf) (in Dutch)

[http://www.privacycommission.be/sites/privacycommission/files/documents/Privacy\\_Act\\_1992.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/Privacy_Act_1992.pdf) (Unofficial English Translation)

The privacy of certain electronic communications is covered by other acts, and the Patients’ Rights Law of 2002 regulates, in part, the use of patient data.

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** The Privacy Commission oversees and enforces the DPL, and can issue recommendations on the application of the DPL.
- 2.2 **Registration.** Every data controller processing personal data by automatic means must notify the Privacy Commission before processing the data; manual processing does not require notification. Automated processing can be exempt from the notification requirement under certain circumstances listed in Articles 51–62 of the Royal Decree of February 13, 2001. These exemptions include processing that is: necessary for payroll management by the employer, used by the employer exclusively for staff management, or necessary to the data controller’s accounting.
- 2.3 Notification can be done online through the Privacy Commission’s website. It can also be done by hard copy. The data controller cannot begin processing until it gets an acknowledgment of receipt of the notification from the Privacy Commission. The acknowledgment is usually sent within three days of receipt. If any of the required information about the processing changes, the data controller must notify the Privacy Commission.
- 2.4 Notification must include the:
  - date of notification and any authority for the automatic processing;

- name and address of the registered offices of the controller and of any representatives in Belgium;
- name of the automatic processing;
- purpose or the set of related purposes of the automatic processing;
- categories of personal data being processed with certain details;
- categories of recipients to whom the data can be disclosed;
- safeguards that must be linked to the disclosure of the data to third parties;
- manner in which the data subjects are informed, the service providing for the exercise of the right to access and the measures taken to facilitate the exercise of that right;
- period of time in which the data may no longer be stored, used or disclosed;
- general description allowing for determination whether the security measures are adequate;
- grounds for the controller's application, if applicable, that certain exceptions may apply; and
- categories of data being transferred to a foreign country, and, for each, the country of final destination (where applicable).

The Commission may require further information, and further notification may be required where the automatic processing is terminated or modified.

### 3. Protected Personal Data

- 3.1 **Personal data** is any information relating to an identified or identifiable natural person. An identifiable person can be identified directly or indirectly, particularly with reference to an identification number or by one or more factors specific to his or her physical, physiological, mental, economic, cultural, or social identity.
- 3.2 The processing of **health-related personal data** is prohibited under Article 7, with a number of exceptions, including the data subject's consent with the understanding that consent can be withdrawn at any time. Health-related data may only be collected from the data subject him- or herself, unless it complies with the King's decree on the conditions for processing of health-related data and is processed under the responsibility of a health professional (save for cases of consent or necessity to prevent danger or criminal offenses).
- 3.3 The processing of personal data relating to disputes that have been submitted to courts and tribunals, as well as to administrative judicial bodies, relating to suspicions, prosecutions or convictions in matters of criminal offenses, administrative sanctions or security measures, is prohibited. However, processing is allowed for persons where it is necessary for the management of their own litigation, by attorneys or other legal advisers where necessary to protect the interests of their clients, and in certain other situations under Article 8, Section 2.
- 3.4 Although Belgium does not have a specific category for **sensitive data**, under Article 6, Section 2, it does prohibit the processing of personal data that reveals a subject's racial or ethnic origin, political opinions, religious or philosophical

beliefs, trade union memberships, and sex life. This prohibition is subject to the following exceptions:

- where the data subject has given written consent with the understanding that consent may be withdrawn at any time;
- where processing is necessary to carry out certain obligations of the data controller under employment law;
- if the data subject has made the data public;
- to protect the vital interests of the data subject;
- for the establishment, exercise or defense of legal claims; or
- if the processing is carried out in the course of legitimate activities by a non-profit organization with a political, philosophical, religious, health-insurance, or trade union-aim and on condition that the processing relates solely to the members of the organization or those in regular contact with them for its purposes so long as the data is not disclosed to a third-party without consent.

#### **4. Data Collection and Processing**

4.1 Generally, data subjects must give unambiguous consent in order for their data to be processed. There are some other exemptions under Article 5 if the processing is necessary:

- for performance of a contract to which the data subject is a party;
- for compliance with an obligation to which the controller is subject by or by virtue of an act, decree or ordinance;
- in order to protect the vital interests of the data subject;
- the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller or in a third party to whom the data is disclosed; or
- for the promotion of the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject claiming protection under the Act.

4.2 Personal data may only be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes, taking into account all relevant factors, in particular, the reasonable expectations of the data subject and the applicable legal and regulatory provisions. Further processing of data for historical, statistical or scientific purposes shall not be considered incompatible.

4.3 When collecting data directly from the data subject, the data controller or the data controller's representative must, with some exception, provide the subject with the name and address of the data controller, the purpose of the processing, and the existence of the right to object on request against the intended processing if the data is obtained for purposes of direct marketing. Unless it is not necessary to guarantee fair processing to the data subject, the data subject must also be provided with the names of the recipients or categories of recipients of the data, whether or not the replies to the questions are obligatory and the consequences

of failure to reply, the existence of the right of access to one's personal data, as well as the right to correct it.

- 4.4 If the data is not collected directly from the data subject, the data controller must still inform the data subject of the information listed above at the time of recording the data. Only where the data is being used for certain public health purposes or is being recorded under legal obligation is the data controller's duty to inform the data subject waived.
- 4.5 The only type of data processing to which the DPL does not apply at all is non-automated processing of personal data that is neither included nor intended to be included in a filing system, defined as any structured set of personal data accessible according to specific criteria. Processing data solely for journalistic, artistic, or literary purposes is also exempt, subject to certain conditions under Article 3, Section 3.

## **5. Data Transfer**

- 5.1 In general, if the data processing is assigned by the data controller to a processor, the data controller must, among other things, agree with the processor that the processor is bound by the same obligations by which the data controller is bound. The data controller is still bound to make sure that data is properly corrected and erased where necessary and to make sure that the processing is taking place in accordance with the DPL.
- 5.2 Transfers within the European Economic Area (EEA) or to a country that otherwise ensures an adequate level of protection are permitted so long as there is compliance with the other provisions of the DPL.
- 5.3 Countries with an adequate level of protection include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.
- 5.4 Transfers outside the EEA that do not ensure an adequate level of protection may still occur if:
  - the data subject has unambiguously consented;
  - the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;
  - the transfer is necessary for the conclusion or performance of a contract between the controller and a third party in the interest of the data subject;
  - the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;
  - the transfer is necessary in order to protect the vital interests of the data subject; or
  - the transfer is made from a register which, according to acts 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 a legitimate interest, to the extent that conditions laid down in law for consultation are fulfilled.

In addition, transfers may be authorized by the Privacy Commission if the controller ensures adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and regarding the exercise of the corresponding rights. Such safeguards can result, in particular, from appropriate contractual clauses.

Authorization may also be gained through the binding corporate rules framework, though special procedures must be met. See <http://www.privacycommission.be/fr/quel-doit-%C3%AAtre-le-contenu-des-r%C3%A8gles-dentreprises-contraignantes-ou-binding-corporate-rules-ou-bcrs>.

The use of EU model contractual clauses is not subject to authorization by the Privacy Commission; however, a copy must still be sent. This processing must be notified on the public register, unless an exception is met. See <http://www.privacycommission.be/en/transfers-outside-the-eu-without-adequate-protection/contractual-clauses>.

## **6. Data Security**

Data controllers must take appropriate technical and organizational measures to protect personal data against accidental or unauthorized destruction, accidental loss, and any alteration, access, or other unauthorized processing of personal data. The security measures must be appropriate, taking into account the state of the art in the field, the cost of implementing security measures, the nature of the data to be protected, and the potential risks.

## **7. Breach Notification**

The DPL does not currently require any obligations concerning breach notification.

## **8. Other Considerations**

There is no legal requirement for companies to appoint data protection officers, although it is recommended to do so by regulations concerning the DPL.

## **9. Enforcement & Penalties**

Violations of the DPL can be prosecuted as a criminal offense resulting in fines ranging from €550 up to €550,000, depending on the offense. Repeat violations are punishable by imprisonment ranging in length from three months to two years. Additionally, a person harmed by violations of the DPL can bring a civil action for damages.



## 1. Applicable Law

At the time of drafting, there is not yet a specific statutory regulation governing data transfers in Brazil, nor is there yet a specific data protection authority. Nevertheless, several laws, as well as the Brazilian Constitution provide Brazilians with some rights with regard to data collection. There are also laws governing protection in specific areas (e.g., bank secrecy, medical ethics, consumer protection, credit, and telecommunications).

The draft Data Protection Bill 2011 has yet to be enacted but may be considered in 2014. The proposed Brazilian legislation is based broadly on the European Data Protection Directive. The draft legislation would require consent prior to transfer and would also require breach notification. The draft legislation also contains a requirement of consent for the transfer of personal data outside of the Brazilian territory. Among other things, it would also establish a Data Protection Authority with the power to issue sanctions and require opt-in consent for sensitive personal data.<sup>2</sup>

Further, Brazil's Internet Law No. 12,965/2014, the "Marco Civil da Internet," was implemented on June 23, 2014. While not a comprehensive data protection or privacy law, the Marco Civil da Internet addresses ISPs, social media websites, search engines, and other online companies hosting user-generated content doing business in Brazil or collecting information from Brazilians, and restricts those parties from sharing user's personal information, communications, and other on-line logging data (while still requiring covered parties to retain certain data and protecting user-related information accordingly).

[http://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm)

## 2. Data Protection Authority and Registration Requirements

Brazil has no data protection authority or database registration requirements.

## 3. Data Collection and Processing

- 3.1 Article 5 of the Brazilian Constitution provides that the "privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages is ensured." Article 5 also grants habeas data. It guarantees the right of privacy and ensures consumers have the right to know what data are held about them and they have the right to correct that data. However, these rights of knowledge and correction under the Constitution currently exist only with respect to records or databases of government agencies or agencies of a public character.

---

<sup>2</sup> A June 2012 report to the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, consulted herein, provides additional analysis of the draft legislation as well as comparison with the patchwork of laws and enforcement of those laws currently in place: See Luiz Costa, "A Brief Analysis of Data Protection Law in Brazil," (June 2012), available at [www.coe.int/t/dghl/standardsetting/dataprotection/tpd\\_documents/Report%20\(June%204th%202012\)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20\(updated%20version\).pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/Report%20(June%204th%202012)%20-%20A%20brief%20analysis%20of%20DP%20in%20Brazil%20(updated%20version).pdf).



- 3.2 The Consumer Protection Law of 1990 regulates consumer databases held by banks, credit agencies, and other companies. “Consumer” is defined broadly under the Law as “any individual or body corporate who acquires or uses any product or service as an end user.” The law requires that any consumer data stored in a database should files be truthful, objective, and easily understood, and prohibits not contain the same piece of the storage of any negative information about a consumer for more than five years. If the consumer did not request that his or her information be stored, the collector must notify the consumer in writing of the inclusion of his or her name in a database. Additionally, consumers are given the right to correct information about themselves. Article 43 of the Consumer Protection Law grants consumers free access of any of their own information stored in a database. It also gives consumers the right to request the prompt correction of an inaccuracy in his information, and requires that the requested correction must be made within five days.

The official text of the Consumer Protection Law is available in Portuguese here: <http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=102415&tipoDocumento=LEI&tipoTexto=PUB>. The Brazilian government has made available an English translation of the Law here:

[http://procon.barretos.sp.gov.br/imagens/legislacao/especifica/lei\\_federal\\_8.0781\\_990/LAW%20N%208078%20AS%20OF%20SEPTEMBER%2011%20-%201990%20-%20Art.%2001%20a%2060.pdf](http://procon.barretos.sp.gov.br/imagens/legislacao/especifica/lei_federal_8.0781_990/LAW%20N%208078%20AS%20OF%20SEPTEMBER%2011%20-%201990%20-%20Art.%2001%20a%2060.pdf) (Part 1);

[http://procon.barretos.sp.gov.br/imagens/legislacao/especifica/lei\\_federal\\_8.0781\\_990/LAW%20N%208078%20AS%20OF%20SEPTEMBER%2011%20-%201990%20-%20Art.%2061%20a%20117.pdf](http://procon.barretos.sp.gov.br/imagens/legislacao/especifica/lei_federal_8.0781_990/LAW%20N%208078%20AS%20OF%20SEPTEMBER%2011%20-%201990%20-%20Art.%2061%20a%20117.pdf) (Part 2)

- 3.3 The Credit Information Law of 2011 imposes several requirements on the creation and access to databases related to credit information. The law forbids the processing of data that is unnecessary in deciding whether to grant credit. This prohibition specifically applies to sensitive data such as political, religious, sexual, and health information. Data subjects have the right to access, rectify, and erase data and be informed of the database manager’s identity and the identity of third parties that will have access to the data. Lastly, the law imposes data quality obligations on the data processors.<sup>3</sup>
- 3.4 The “Marco Civil” draft law became a priority for the Brazilian government in late-2013 following Edward Snowden’s revelation of the NSA’s PRISM program. The Marco Civil is aimed at defining core rights of the Internet—including freedom of access, expression, privacy, and data protection. However, recent amendments to the Marco Civil added after the NSA PRISM scandal broke may also have serious implications for companies doing business in Brazil. These amendments would require companies to use local data storage centers to store data on their Brazilian users. Companies could not transfer personal information of Brazilians outside of Brazil for storage or processing. Jan 1, 2014 the Marco Civil has not been passed.

---

<sup>3</sup> See *id.*

#### **4. Data Transfer**

Sectoral laws sometimes expressly provide for transfer on consent. For example, a patient's medical information may be disclosed by his or her doctor for a number of reasons that include the patient's consent. However, there is no general law expressly requiring that data subjects provide consent for disclosure of their information, whether the transfer is domestic or international.

Nevertheless, given the sectoral laws and overall principles described herein, as well as the broad consumer protection principles and the fact that privacy is a constitutional right, consent is required unless otherwise indicated by law.

#### **5. Data Security**

While Brazil's broad principles regarding privacy place responsibility on data controllers to protect private data, Brazil has no specific data security requirements in place with general applicability.

#### **6. Breach Notification**

Brazil has no data breach notification laws currently in place, though as stated above the draft legislation would require it.

#### **7. Enforcement & Penalties**

In Brazil, liability for unauthorized disclosure of personal data can take place through civil law suits and/or administrative actions brought by individuals or certain public authorities. The disclosure of private or confidential information may be considered a crime under the Brazilian Criminal Code<sup>4</sup>

Under the Consumer Protection Law, the failure to immediately correct inaccurate information in a database is considered a criminal infraction, punishable by one to six months' imprisonment or a fine. A violation of the Consumer Protection Law may also result in administrative sanctions of between UFIR 200 - 3,000,000.

---

<sup>4</sup> Westlaw Business Laws of Brazil § 17:58.

## 1. Applicable Law

Data protection laws and protections stem from numerous federal, provincial and local statutes and regulations in Canada, creating a complex system of data privacy protections and enforcement mechanisms. These laws cover a wide swath of issues in the private, public and health sectors. This summary focuses on the primary laws applicable to the private sector. The Canadian federal law is the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (“PIPEDA”).

<http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html>

The focus of this summary is on PIPEDA; however, privacy legislation applicable to the private sector in Alberta, British Columbia, and Quebec has been declared substantially similar to PIPEDA: Alberta’s Personal Information Protection Act, British Columbia’s Personal Information Protection Act, and Quebec’s Act Respecting the Protection of Personal Information in the Private Sector. For ease of reference, this summary will refer to these statutes combined with PIPEDA as the “Canadian Data Protection Statutes.”

Generally, PIPEDA applies to organizations subject to federal regulations (e.g., banks, airlines, railways), commercial organizations operating wholly in a province that has not enacted its own private sector privacy legislation (i.e., not British Columbia, Alberta, or Quebec) and to inter-provincial and international collection, use, and disclosure of personal information.

## 2. Data Protection Authority and Registration

2.1 **Federal Authority.** Under PIPEDA, the Office of the Privacy Commission of Canada (“Commissioner”), an Officer of Parliament who reports directly to the federal Canadian House of Commons and Senate, is charged with overseeing PIPEDA.

- In this role, the Commissioner has the following responsibilities and powers:
  - investigates complaints of PIPEDA violations;
  - initiates complaints of violations of PIPEDA as necessary;
  - reports to Parliament on privacy issues;
  - audits organizations subject to the PIPEDA so as to advise on compliance;
  - conducts privacy-related research; and
  - engages in public education concerning privacy issues.
- The Commissioner does not, however, have any direct power to impose fines or make remedial orders for violations of the PIPEDA, although the Commissioner may bring complaints through applications to the Federal Court. The Federal Court can find violations, award damages, and issue injunctive relief.

2.2 **Provincial Authority.** Each provincial privacy commissioner or its equivalent has responsibilities and powers similar to that of the Commissioner. Unlike the Commissioner, however, some of the provincial commissioners may issue orders

to ensure compliance. The website of the Commissioner contains helpful links to the laws and relevant authorities at the provincial level, at [http://www.priv.gc.ca/resource/prov/index\\_e.asp](http://www.priv.gc.ca/resource/prov/index_e.asp).

2.3 **Registration.** There are no registration requirements.

### 3. Protected Personal Data

3.1 Under PIPEDA, “**personal information**” means “information about an identifiable individual,” but it does not include the name, title or business address or telephone number of an employee of an organization.”

3.2 Although there is no separate definition for any particularly **sensitive personal information**, PIPEDA does recognize that some personal information is more sensitive than others and mandates more strict compliance requirements with respect to that more sensitive data.

### 4. Data Collection and Processing

4.1 The Canadian Data Protection Statutes generally require that organizations subject to these laws only collect, use and disclose personal information for “purposes that a reasonable person would consider are appropriate in the circumstances.” The Canadian Data Protection Statutes generally, and subject to certain exceptions, require an individual’s consent prior to the collection, use, and disclosure of the individual’s personal information. (The exceptions are different as to each of “collection,” “use,” and “disclosure” without knowledge or consent.) An organization must also make reasonable efforts to ensure that the individual is advised of the purposes for which that individual’s consent may or will be used and those purposes must be stated in a reasonably understandable manner.

4.2 PIPEDA provides exceptions for *collection* without knowledge or consent if:

- the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
- the collection is solely for journalistic, artistic or literary purposes;
- the information is publicly available and is specified by the regulations; or
- the collection is made for the purpose of making certain disclosures.

4.3 PIPEDA provides exceptions for *use* without knowledge or consent, if:

- in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed,

and the information is used for the purpose of investigating that contravention;

- it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
- it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;
- it is publicly available and is specified by the regulations; or
- it was collected under certain of the exceptions to the rule regarding collection without knowledge or consent.

4.4 PIPEDA provides exceptions for *disclosure* without knowledge or consent, if the disclosure is:

- made to a barrister, solicitor, or notary who is representing the disclosing organization;
- for the purpose of collecting a debt owed by the individual to the organization;
- required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with the rules of court relating to the production of records;
- made to a government institution under certain circumstances, for example, breach of a government agreement, national security, and the conduct of international affairs;
- made to protect the life, health or security of a person or persons in an emergency;
- for statistical or scholarly research purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent, and the Commissioner is informed;
- made to an institution whose function includes the conservation of records or archival importance;
- made after the earlier of (i) one hundred years after the record was created or (2) twenty years after the death of the individual whom the information is about; or
- required by law.

4.5 Generally, there is a more flexible standard for consent under PIPEDA, and consent may be either implicit or explicit, oral, or in writing, including through electronic means. Some of the provincial laws also provide for this more flexible standard for obtaining consent.

4.6 The Canadian Data Protection Statutes generally require that organizations identify the purposes for which personal information will be collected at or before the time of collection and make available the organization's personal information collection, use, and disclosure practices.

- 4.7 The Canadian Data Protection Statutes generally allow individuals the right to access personal information held by an organization (subject to certain exceptions) and to correct any inaccuracies or required updates concerning the personal information held by the organization. Organizations also are obligated to ensure personal information is accurate and complete, particularly where that information will be disclosed outside of the organization, and/or where an individual's personal information will be used to make a decision concerning the individual.
- 4.8 Special Considerations Regarding Employee Data: Under the Canadian Data Protection Statutes, the collection, use, and disclosure of employee personal information is generally subject to the same rules. There are, however, often more strict consent requirements in the employment context due to the nature of the employee/employer relationship. In the employment context, PIPEDA only applies to employees of organizations subject to federal regulations and, thus, does not apply to employees in provinces without any employee privacy legislation.

## 5. Data Transfer

- 5.1 Generally, when an organization transfers personal information outside of the organization, it remains responsible for the protection of the personal information and ensuring compliance with the applicable statutes. Stricter, more specific requirements under the provincial laws also may apply to data transfers, particularly if transferring outside of Canada.
- 5.2 PIPEDA itself does not distinguish between international and domestic transfer. Therefore, in accordance with the principles on the *use* of data under PIPEDA, so long as the transfer is consistent with the use for which the data was originally collected, consent to transfer the data is not required. If not, consent would be required. The Commissioner has issued best practice guidance on the issue of cross-border transfers, available at [http://www.priv.gc.ca/information/guide/2009/ql\\_dab\\_090127\\_e.asp](http://www.priv.gc.ca/information/guide/2009/ql_dab_090127_e.asp), that indicates as much. It also stresses transparency, and that "organizations need to make plain to individuals that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction. They must do this in clear and understandable language. Ideally they should do it at the time the information is collected."
- 5.3 Service Providers. The Canadian Data Protection Statutes generally allow organizations to transfer personal information to third-party service providers, subject to certain additional requirements. Organizations must ensure the same level of protection by a third party through contractual agreement or otherwise. These contractual agreements typically require adherence to the Canadian Data Protection Statutes and may include indemnification provisions, liquidated damages, and other relief in the event the third party fails to comply with privacy law requirements.
- 5.4 Transfer to Service Providers Outside Canada. There are also provisions in some of the statutes specifically concerning outsourcing personal information outside of Canada or, in some circumstances, outside of a particular province.

For example, in addition to other required notices, Alberta requires that an organization that (a) uses a service provider outside of Canada to collect personal information about an individual that was collected with consent, or (b) that indirectly or directly transfers personal information that was collected with consent to a service provider outside of Canada, must, before or at the time of collecting or transferring the information, notify the individual:

- the way in which the individual may obtain access to written information about the organization'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 organization 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 organization.

See, Personal Information Protection Act, SA 2003, c P-6.5, at <http://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html>

## **6. Data Security**

- 6.1 The Canadian Data Protection Statutes require that organizations appoint a position/individual who is responsible for the organization's compliance with the requirements under the various applicable laws.
- 6.2 The Canadian Data Protection Statutes require reasonable measures to protect personal information against theft, other loss, and unauthorized collection, access, disclosure, copying, use, destruction, or modification.

## **7. Breach Notification**

- 7.1 PIPEDA does not contain specific breach notification requirements, although proposed legislation amending PIPEDA includes certain breach notification requirements and was introduced for consideration in both 2012 and 2013.
- 7.2 Alberta's privacy legislation contains certain breach notification requirements. Pursuant to Alberta's law, an organization must provide written notice to the Commissioner without unreasonable delay concerning any incident involving the loss or unauthorized access to or disclosure of personal information where a reasonable person would consider that a real risk of significant harm to an individual exists. The Commissioner may require the organization to notify the individuals to whom there is a real risk of significant harm directly.

## **8. Enforcement & Penalties**

- 8.1 Under PIPEDA, when a complaint is filed, the Commissioner must conduct an investigation and issue findings and a recommendation. Once the Commissioner's report is issued, the complainant may apply to the Federal Court for a *de novo* review of the findings and, as explained above, the Federal Court may issue an order requiring compliance, damages and/or injunctive relief. The organization that is the subject of the complaint may not seek review by the Federal Court (meaning only the complainant may seek review).



- 8.2 Each provincial privacy commissioner or its equivalent has responsibilities and powers similar to that of the Commissioner. Unlike the Commissioner, however, some of the provincial commissioners may issue orders to ensure compliance. Some of the provincial laws (*i.e.*, Alberta and British Columbia) provide for specific offenses under the provincial laws including, but not limited to, obstructing a commissioner's investigation, retaliation, destroying information to avoid compliance, and failing to comply with a commissioner's order. These violations are punishable by major fines, including not more than \$100,000 for non-individual violations. Some provincial laws also provide for private rights of actions against a non-complying organization for damages.
- 8.3 Although class action lawsuits related to data privacy breaches have been initiated in Canada, they have been mostly unsuccessful, with a few notable and recent exceptions. The lack of success likely relates to numerous reasons, two of which being the fact that a right of action under the federal law only arises after a full investigation and recommendation by the Commissioner and the fact that class action litigation is subject to more stringent requirements under Canadian law.



## 1. Applicable Law

Data privacy in Chile is currently governed by the Law for the Protection of Private Life, Law No.19,628 (1999), and its most recent update, Law No. 19,812 (2002), Decree No. 779 (2000), the Law on Access to Public Information, Law No. 20,285 (2008), and Decree No. 13 (2009), implementing Law No. 20,285. In that same order, these are available at:

<http://www.leychile.cl/Navegar?idNorma=141599>

<http://www.leychile.cl/Navegar?idNorma=199093>

[http://www.registrocivil.cl/transparencia/marcoNormativo/DTO\\_779.pdf](http://www.registrocivil.cl/transparencia/marcoNormativo/DTO_779.pdf)

<http://www.leychile.cl/Navegar?idNorma=276363>

<http://www.leychile.cl/Navegar?idNorma=1001095>

While Chile's data privacy rules have remained static for some time, in December 2014, Chile's Deputy Economy Minister indicated that [Chile would soon introduce legislation to create an autonomous National Council for Data Protection](#) to oversee data protection issues, fix enforcement laws, and impose fines of up to 432 million Chilean Pesos for infractions.

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** At this time, Chile has not yet established a government agency responsible for overseeing compliance with Chile's data protection law. Any violations must be brought by an individual to the attention of the Jueces de Letras for the protection of his or her rights.
- 2.2 **Registration.** Only databases containing personal data held by public entities must be registered. This registry is maintained by the Servicio de Registro Civil.

## 3. Protected Personal Data

- 3.1 **Personal data** is defined as any information concerning identified or identifiable natural persons.
- 3.2 **Sensitive personal data** is defined as personal data regarding the physical or moral characteristics of an individual, facts or circumstances of an individual's private life or intimate information, such as personal habits, race, beliefs or religion, political opinions, ideologies, physical or psychological information, and sexual information.

## 4. Data Collection and Processing

- 4.1 Personal data can only be collected:
  - when the data subject gives express consent;

- In order for an individual to give consent, the entity collecting the data must inform the individual of the purpose of collection, and whether the information will be shared with third-parties.
- when the data are collected from public sources;
- when explicitly authorized by law;
- when the data are economic, financial or commercial data (though special obligations will then apply);
- when the information is contained in listings related to a category, and only discloses any relation to the specific group, e.g., professional activity, education;
- by a private entity for its own use; or
- by entities associated with any of the above, when used for statistical purposes, for the benefit of its associates.

#### 4.2 Special Considerations Regarding Sensitive Data

Sensitive data may only be collected when expressly authorized by law, by consent of the individual, or for the purpose of providing health benefits. In order for an individual to give consent, the entity collecting the data must inform the individual of the purpose of collection, and whether the information will be shared with third parties. Sensitive data can be collected and processed if authorized by law to accomplish a compelling public interest.

### 5. Data Transfer

There are no general provisions on data transfer, although the possibility of transfer to third-parties is part of what must be disclosed to obtain consent. With specific regard to commercial, financial, banking, and credit-related personal information, Articles 17 and 18 of Law 19628 provides that collectors cannot disclose that data unless it is included in promissory notes, in mortgage delinquency cases, and certain other situations, including any in which the government requires disclosure. Disclosure of commercial, financial, banking, or credit-related information must be done within five years after the data subject becomes delinquent; otherwise, disclosure is prohibited after the five years. Moreover, they cannot continue to communicate this information once the obligations have been extinguished or otherwise provided by law. Public and private entities that provide gas, electricity, water, and phone services cannot disclose personal information even in the case of delinquent accounts.

### 6. Data Security

A party is responsible for the protection of any database that contains personal data, though the data protection law does not specify any particular security requirements. The law does mandate that any employee who handles personal information, at either public or private entities, keep confidential any information, even after termination of employment.

### 7. Breach Notification

Currently, there is no breach notification requirement.

## **8. Other Considerations**

Individuals have a right of access and are entitled to information from public or private entities:

- the data collected;
- its origin and recipients;
- the purpose for the storage of the data; and
- the identity of persons or bodies to which the data is transmitted.

An individual's right to request access to, modification of, deletion of, or to block use of personal data, cannot be limited by any act or agreement (except in some limited instances such as national security).

## **9. Enforcement & Penalties**

Enforcement is through civil suits by affected individuals. Under Article 23 of Law 19,628, the private person or entity or body responsible for the database must compensate for property and moral damage caused by the improper treatment of the data. The amount of compensation is to be determined by the judge given the severity of the facts.

For breaches of Articles 17 and 18 of Law 19,628—the provisions regard to commercial, financial, banking, and credit-related personal information—fines of between 1-10 month's salary or 10-50 UTM may be imposed. Under Article 16 of Law 19,628, a lack of timely delivery of information in response to an access request or a delay in making a requested change can be punished by 2 to 50 UTM, and if the database is a public body, the court may make suspensions for a period of 5-15 days.

---

# China (People's Republic)

## 1. Applicable Law

China does not yet have comprehensive national legislation regulating data privacy. Currently, privacy breaches, when they are addressed, are handled through PRC Tort Law, PRC Criminal Law, or a variety of local ordinances (for example, Shanghai's Consumer Protection Rules provide some guidance on data privacy).

Several recently passed regulations, however, are of note for companies doing business in China, particularly business concerning Internet services.

On December 29, 2011, China's Ministry of Industry and Information Technology ("MIIT") promulgated the Several Regulations on Standardizing Market Order for Internet Information Services, <http://www.miit.gov.cn/n11293472/n11293832/n12771663/14417081.html> (in Chinese). These regulations took effect March 15, 2012, and create several nationwide privacy standards specific to "Internet Information Service Providers" ("IISPs"). The following sections outline the effect these regulations have on IISPs that do business in China.

[http://www.loc.gov/lawweb/servlet/lloc\\_news?disp3\\_l205403038\\_text](http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403038_text)

On December 28, 2012, China's Standing Committee of the National People's Congress ("NPC") issued a decision strengthening online personal data protection ("Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data") ("2012 Directive"), [http://www.gov.cn/jrzq/2012-12/28/content\\_2301231.htm](http://www.gov.cn/jrzq/2012-12/28/content_2301231.htm) (in Chinese). The Standing Committee has stated that it expects to amend all previously passed regulations relating to the Internet based on this new regulation.

[http://www.loc.gov/lawweb/servlet/lloc\\_news?disp1\\_l205403445\\_text](http://www.loc.gov/lawweb/servlet/lloc_news?disp1_l205403445_text)

The NPC revised the Consumer Protection Act on October 25, 2013, which took effect on March, 15, 2014 (the "Act"), <http://www.chinalaw.gov.cn/article/fgkd/xfq/fl/201310/20131000392972.shtml> (in Chinese). In response (in part) to increases in online shopping, business operators now face heavier obligations to protect the personal information of the consumer, including obligations to (i) inform consumers of the purpose, method, and scope of the collection of their personal information while seeking consent from the consumer before collection; (ii) publish internal business rules with respect to the collection and use of the consumer's personal information; and (iii) take precautions to protect consumers' personal information and not disclosing, selling, or providing that information to third parties.

China also has separate sector laws addressing Personal Information Protection of Telecom and Internet Users ("MIIT Regulation"); Administrative Measures for Online Transactions; and Medical Records Administration Measures of Medical Institutions and Measures for Administration of Population Health Information ("PHI Measures").

There is no omnibus framework for the intersection of these rules; therefore, each is addressed categorically and separately below.

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** There is no national data protection agency. The Ministry of Industry and Information Technology is the responsible authority for regulating IISPs.
- 2.2 Under the 2012 Directive, “Supervising Departments” are empowered to take measures to prevent, stop, or punish those who infringe on online privacy, obtain personal digital information through illegal means, or sell or illegally provide information to others, and IISPs are required to give assistance during investigations.
- 2.3 **Registration.** There is no registration requirement.

## 3. Protected Personal Data

**Personal data** or “**User’s Personal Information**” (“UPI”), as it is referred to in the regulations, is defined broadly as any information that allows a user to be identified when used alone or in conjunction with other information. There is no statutory definition of sensitive personal data.

Under the 2012 Directive, electronic information by which the individual identity of citizens can be distinguished is protected. China’s MIIT Regulation provides the same definition, but also encompasses information collected by telecom business operators and ISPs concerning the time and location of users’ use of services.

The NPC revisions to the Act apply to both information that identifies individual citizens as well as electronic information relating to the personal privacy of PRC citizens.

## 4. Data Collected and Processing

IISPs must obtain all users’ consent before collecting any UPI through their Internet services. IISPs are required to disclose the types of UPI they collect, the purpose of the collection, and the method through which it is collected. All UPI collected must be for the purpose of aiding the IISPs in providing services.

Under the 2012 Directive, IISPs and other organizations that collect or use citizens’ individual electronic information during their business activities, shall abide by the principles of legality, legitimacy and necessity, clearly indicate the objective, methods and scope for collection and use of information, and obtain agreement from the person whose data is collected. Further, such entities must make public their collection and use rules.

## 5. Data Transfer

IISPs must obtain all users’ consent before sharing UPI with third parties.

Under the 2012 Directive, Network service providers and other organizations must strictly preserve the secrecy of collected electronic information, they may not divulge, distort, or damage it, and they may not sell or illegally provide it to other persons.

China is not a party to any treaty with the EU or any nation in a EU-U.S. safe harbor-type framework.

## **6. Data Security**

IISPs are required to securely store all data they collect in order to prevent disclosure to unauthorized parties.

Under the 2012 Directive, IISPs and other organizations must adopt technological measures and other necessary measures to ensure information security and prevent citizens' individual electronic information from being divulged, damaged or lost. When divulged, damaged, or lost, responsible parties will immediately adopt remedial measures.

## **7. Breach Notification**

If a breach of UPI should occur, IISPs are required to take steps to minimize any adverse consequences and prevent further disclosure. Furthermore, if there is a risk of serious consequences IISPs must report the breach to authorities.

Under the 2012 Directive, where unlawful information is published or disseminated, IISPs and other organizations shall cease the dissemination of the said information, delete it, preserve relevant records, and inform relevant controlling departments.

## **8. Special Considerations**

Under the 2012 Directive, Internet users must use their real names to identify themselves to service providers, including Internet or telecommunications operators.

## **9. Enforcement and Penalties**

IISPs that violate these regulations are normally subject to penalties ranging from RMB10,000 to RMB30,000. However, recent Supreme Court guidance indicates that a victim of infringement of rights may be compensated up to RMB

Under the 2012 Directive, violators are subject to liability including warnings, fines, confiscation of unlawful income, cancellation of permits or cancellation of fines, closure of websites, prohibition of relevant responsible personnel from future engagement in the network service business, and other civil, administrative and even criminal punishments. Violations may also be recorded in the "social credibility files" and be made public. On August 8, 2014, a Shanghai court found a British couple guilty of illegal collection of personal information, fining the husband Peter Humphrey RMB200,000 and sentencing him to two and a half years in prison; his wife was fined RMB150,000 and sentenced to two years. Humphrey was also sentenced to deportation after finishing his term.

## 1. Applicable Law

Colombia's new law on data protection, passed in 2010, received approval from the Constitutional Court in Colombia on October 7, 2011. With a few exceptions, most provisions of Bill Number 185 of 2010 Statutory Senate 046, 2010 Camera, were approved. The law entitled *Ley 1581 del 17 de Octubre de 2012 por el cual se Dictan Disposiciones Generales para la Protección de Datos Personales* was formally enacted on October 17, 2012 (the "Act").

<http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf>

On April 18, 2013, the Act officially came into effect after a six month grace period for companies to come into compliance. In late June 2013, implementing regulations for the Act were published by the [Colombian government](#). The implementing regulations, in Spanish, are available here:

[http://op.bna.com/pl.nsf/id/dapn-99bhje/\\$File/colombia.pdf](http://op.bna.com/pl.nsf/id/dapn-99bhje/$File/colombia.pdf)

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** La Superintendencia de Industria y Comercio ("Superintendency").

2.2 **Registration.** The Superintendency manages the National Public Registry of Databases. The Act does not itself dictate the registration requirements, but instead directs the Government to pass a regulation within one year that dictates what information and which databases must be included in the registry.

## 3. Protected Personal Data

3.1 **Personal data** is any information relating to an identified natural person.

3.2 **Sensitive personal data** is data that affects the privacy of the data owner or the abuse of which may lead to discrimination against them, such as data that reveals racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in a trade union, social organization, human rights or to promote interests of any political party or to guarantee the rights and guarantees of political opposition parties, health information, information on sexual life and biometric data.

## 4. Data Collection and Processing

4.1 The data subject of personal data must give prior, informed consent before any collection occurs. In order to give informed consent, the data subject must be informed of:

- the data collected;
- the purpose of the collection;



- the identity and address of the data controller; and
- the data subject's rights including access rights, the right to update and correct personal data, and the right to revoke consent.

4.2 The processing of sensitive data is prohibited except where:

- the data subject has given his/her explicit consent, except in cases where such consent is not required under this law;
- the processing of the data is necessary to protect the vital interests of the data subject and the data subject is physically or legally incapacitated. In this situation, the permission of the data subject's legal representative is required;
- the processing is carried out in the course of the legitimate activities, with appropriate guarantees, by a foundation, NGO, association, or any other non-profit, with a political, philosophical, religious or trade union purpose, provided that data relates exclusively to its members or to persons who have regular contact with the organization because of its purpose. In these events, the data cannot be given to third parties without the consent of the data subject;
- the processing relates to data that are necessary for the establishment, exercise, or defense of a right in a trial; or
- the processing has a historical, statistical, or scientific purpose.

## 5. Data Transfer

5.1 Generally, the transfer of data to any countries that do not provide appropriate levels of protection as determined by the Superintendency is prohibited. The following exceptions apply:

- the subject of the data has given express and unequivocal consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data controller;
- the exchange of medical data, when required for reasons of public health or hygiene;
- transfers agreed upon in international treaties to which Colombia is a party;
- transfers legally required to safeguard the public interest; or
- the Superintendency approves of the transfer.

## 6. Data Security

While the data protection law does not specify the type of security measures to adopt and implement for the safeguarding of personal data, appropriate technical and organizational measures must be taken that are aimed at ensuring the integrity, confidentiality, and availability of the data.



## **7. Breach Notification**

An injured party must be notified whenever anyone in charge of a database learns of a security breach that has the potential of affecting the rights of the injured parties in a significant way.

## **8. Other Considerations**

8.1 The subjects of personal data have the following rights:

- the right to know, update, and correct their personal data;
- the right to request proof of consent granted to the data processor, unless consent is not required under this law;
- the right to be informed by the data processor of how the personal data was used;
- the right to submit complaints of violations of data processing law to the data processing authority;
- the right to revoke consent and/or request the removal of data which is processed in a manner that does not comply with the constitutional and legal principles, rights, and guarantees; and
- the right to free access of their processed personal data.

8.2 The processing of personal data of children and adolescents is outlawed unless it is public in nature.

## **9. Enforcement & Penalties**

The Superintendency may impose the following penalties on data controllers and processors:

- a fine of up to 2,000 times the monthly minimum wage at the time of the imposition of the penalty;
- suspension of database use for up to six months;
- temporary closure of the operations related to the database; or
- immediate and definitive closing of a transaction involving the use of sensitive data.

## 1. Applicable Law

In Costa Rica, data privacy is governed by the *Ley Protección de la Persona frente al Tratamiento de sus Datos Personales* (Law of Protection of the Person in the Processing of His Personal Data) (the “Law”), Law 8968, enacted on September 5, 2011, as well as the *Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales* (Regulations of the Law of Protection of the Person in the Processing of His Personal Data) (the “Regulations”), published March 5, 2013. This law and its regulations apply to both automatic and manual processing of data in the private and public sectors. Databases made for internal (in-house) or personal use are not covered by this law.

<http://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf> (Spanish version of Law).

[http://www.redipd.org/legislacion/common/legislacion/costa\\_rica/Decreto\\_37554JP20102012ReglamentoCostaRica.pdf](http://www.redipd.org/legislacion/common/legislacion/costa_rica/Decreto_37554JP20102012ReglamentoCostaRica.pdf) (Spanish version of Regulations).

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** Agencia de Protección de Datos de los habitantes (“Prodhab”).
- 2.2 **Registration.** All databases, public and private, administered for the purposes of distribution, disclosure, or business administration must register with Prodhab.
- 2.3 **“Superuser” Account.** All data managers must provide Prodhab with access to their database through a “superuser” account. This account must allow unrestricted access to the database in the event of a complaint or in the event Prodhab receives evidence of wrongful data management.

## 3. Protected Personal Data

- 3.1 **Personal data** is any information relating to an identified or identifiable natural person.
- 3.2 **Sensitive personal data** is information revealing racial origin, political opinions, religious or spiritual beliefs, socioeconomic status, genetic information, or sexual orientation.

## 4. Data Collection and Processing

- 4.1 In order to collect personal data, a data controller must obtain written (physical or electronic) consent from the data subject after informing the data subject of:
  - the existence of the database;
  - the intended purpose of the data collection;
  - the destination of the information and who can view it;

- whether or not the questions asked to collect data are required or optional;
  - the consequences of a refusal to provide data;
  - the ability to exercise their rights; and
  - the identity and address of the data controller.
- 4.2 Consent is not necessary when required by law or where the data is obtained from public sources.
- 4.3 Consent may be freely revoked. Data managers have three business days to acknowledge and five business days to comply with the revocation of consent.
- 4.4 Special Considerations Regarding Sensitive Data

No person can be required to provide sensitive data. The processing of sensitive data is prohibited unless:

- the data processing is carried out during the course of the legitimate activities of a foundation, association, or other body with a political, philosophical, religious, or trade union purpose, and the data solely relates to members or people who have regular contact with the organization;
- the processing is to protect the vital interests of another person or, in the event that the person concerned is incapable of consent;
- the processing relates to data that the person concerned has released voluntarily;
- the processing is necessary for the establishment, exercise, or defense of a right in a judicial proceeding; or
- the processing is necessary to the provision of medical care and performed by someone with an obligation to keep the data confidential.

## **5. Data Transfer**

The data processor (whether public or private sector) may only transfer data when the individual has consented explicitly and validly to the transfer and such transfer was made without violating the principles and obligations under the law. Data managers must establish a contract with data transferors to ensure the transferor is held to at least the same standards as the data manager.

## **6. Data Security**

The user of data files must take such technical and organizational measures as are necessary to guarantee the security of personal data in order to avoid their alteration, loss, and unauthorized access. The regulations establish certain minimum protocols that must be implemented and registered with Prohab:

Minimum protocols include:

- 1) Developing policies and manuals concerning data privacy and protection;
- 2) implementing a training manual and procedure regarding staff awareness on the protection of personal data;

- 3) establishing procedures to respond to complaints and questions, as well as requests to access, amend, modify, block, or delete a data owners data or to revoke consent for processing;
- 4) creating measures and technical procedures to maintain a record of personal data during processing; and
- 5) establishing procedures to inform any transferors of data of the data security obligations required.

The specific security measures taken shall consider the following factors:

- 1) The sensitivity of the personal data processed;
- 2) the technology used for processing;
- 3) potential consequences of a violation of privacy in the data;
- 4) the number of holders of personal data;
- 5) previous vulnerabilities; and
- 6) any other factors that may be applicable.

Data managers may contract or subcontract with a service provider as long as they do not process personal data. It is the data manager's responsibility to ensure the contractor meets the minimum security requirements.

## **7. Breach Notification**

Data managers must inform data owners of any irregularities in the processing or storage of data, such as loss, destruction, or theft due to a security vulnerability. Managers must notify any affected party within 5 days of the incident. Data managers must also conduct a thorough process of review during those 5 days to determine the cause of the data incident. Finally, data managers must notify Prohab of the incident, however, there is no specific timeline for this notification.

Any notice provided must contain information regarding:

- 1) The nature of the incident;
- 2) the personal data compromised;
- 3) the corrective actions that have been taken; and
- 4) instructions for obtaining further information about the incident.

## **8. Other Considerations**

Habeas data is a right incorporated into Costa Rica's data protection law that allows an individual to have access to any data about them contained in a database. Every person has the right to obtain the data about them found in public or private databases and they may also request that the data be removed, updated, or rectified if it can be proven to be incorrect or confidential.

"Right to be forgotten." Personal data may not be retained for a period longer than ten years after the event in which it is collected occurs. The only exception to this is if there exists an agreement between the parties specifying a longer period, or if there is a law allowing longer retention. If it is necessary to retain any data longer than 10 years, it must be rendered anonymous.

## **9. Enforcement & Penalties**

Private citizens can bring suit in court where their rights to privacy or data protection have been violated. Prodhav can investigate database malfeasance on its own initiative or upon receiving a complaint from a citizen. Prodhav's power to impose sanctions is without prejudice to the corresponding criminal penalties. Criminal prosecutors may also bring actions on behalf of individuals for the misuse of intimate or private data, a crime punishable by up to three years' imprisonment if the defendant is responsible for the data. Data processors can also be subject to fines ranging from fifteen to thirty "base salaries" and a suspension from database use of up to six months.

Serious offenses under the law include, for example, transfer to databases in other countries without the consent of the data owner and processing data without being registered with Prodhav.

## 1. Applicable Law

In the Czech Republic, data privacy is governed by Act No. 101/2000 Coll. on the Protection of Personal Data, available in English at <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en> (the “Act”). The Act came into force on June 1, 2000.

The Act applies to the processing of personal data, by automatic and manual means, by state authorities, territorial self-administration bodies, other public authority bodies, and natural and legal persons. The Act also applies (i) where the data controller is not established in the Czech Republic, where Czech law is applicable by virtue of public international law and (ii) where the data controller is not established in the EU, but uses equipment situated in the Czech Republic to process personal data (other than for the purposes of transit).

The Act does not apply to personal data processing carried out by a natural person for personal purposes or to accidental personal data collection, unless the data are subject to further processing.

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Office for Personal Data Protection (“Office”).

2.2 **Registration.** Generally, all data controllers and processors must register with the Office prior to conducting their activities.

2.3 The registration requirement does not apply to processing of personal data:

- that are part of data files made publically available by special Act;
- imposed on the controller by a special Act or when such data are needed for exercising rights and obligations arising out of a special Act; and
- that with the consent of the data subject, pursues political, philosophical, religious or trade-union aims carried out within the scope of the legitimate activities of the association and which relates only to members of the association or persons with whom the association is in common contact.

2.4 The notification must include the following information:

- the name, date of birth and address of the data controller or in the case of an entity, its trade, corporate name, seat and identification number, and the names of its statutory representatives;
- the purpose or purposes of processing;
- the categories of data subjects and of personal data pertaining to these subjects;
- the sources of personal data;
- the description of the manner of personal data processing;
- the location or locations of personal data processing;
- the recipient or category of recipients;
- the anticipated personal data transfers to other countries; and

- the description of measures adopted for ensuring the protection of personal data.

2.5 Processing generally may begin after 30 days from the delivery of the notification.

### 3. Protected Personal Data

3.1 **Personal data** is defined as any information relating to an identified or identifiable data subject.

3.2 **Sensitive personal data** is defined as personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, criminal convictions, health status and sexual life of the data subject, genetic data of the data subject, and biometric data permitting direct identification or authentication of the data subject.

### 4. Data Collection and Processing

4.1 The data controller is subject to a number of obligations, including that it must: (i) collect and process data only according to a specified purpose and to the extent necessary to fulfill that purpose; (ii) process only accurate personal data; (iii) preserve data only for a period of time necessary for its processing; (iv) ensure that data collected for different purposes are not grouped; (v) collect personal data in an open manner and without pretext of some other purpose; and (vi) specify the means, manner, and purpose for which the data are to be processed.

4.2 When collecting personal data, the data controller must inform the data subject of:

- the scope of the processing and purpose(s) for which the personal data shall be processed,
- who will process the personal data, and in what manner; and
- to whom the personal data may be disclosed.

This is the case unless the data subject is already aware of this information. In addition, the data controller must inform the data subject about his right of access to the personal data, the right to have his personal data rectified as well as other rights where the data subject finds or presumes that the controller or processor is carrying out processing of his or her personal data in contradiction to the protection of his or her private life or the law.

4.3 If the data was not obtained from the data subject, the controller need not provide the above information, if (i) under certain conditions if he is processing data exclusively for statistical, scientific, or archival purposes; (ii) the data is necessary to exercise the rights and obligations under special Acts; (iii) the processing is of lawfully published data; or (iv) processing is done with the consent of the data subject.

- 4.4 Where the controller processes personal data obtained from the data subject, he is obliged to instruct the data subject on whether the provision of the personal data is voluntary or obligatory.
- 4.5 Where the data subject is obliged to provide the personal data pursuant to a special Act, the controller shall instruct the data subject on this fact and on the consequences of refusing to provide the personal data.
- 4.6 Generally, a controller may process data only with the consent of the data subject. When giving consent, the data subject must be provided with the information about the data being processed, the purpose of the processing, the identity of the controller and the time period for which the consent is given.
- 4.7 In the absence of consent from the data subject, a data controller may only process personal data if:
- it is carrying out processing, which is essential to comply with the legal obligations of the data controller;
  - the processing is essential for fulfillment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the data subject;
  - the processing is essential for the protection of vitally important interests of the data subject;
  - the processing is in relation to personal data that were lawfully published in accordance with special legislation;
  - the processing is essential for the protection of rights and legitimate interests of the controller, recipient or other person concerned;
  - it provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity or their functional or working position; or
  - the processing relates exclusively to archival purposes pursuant to a special Act.
- 4.8 Sensitive data may only be processed where:
- the data subject has given express informed consent;
  - it is necessary in order to preserve the life or health of the data subject or some other person or to eliminate imminent serious danger to their property;
  - it is in connection with ensuring health care, public health protection, health insurance, and the exercise of public administration in the health sector or it is related to assessment of health in other cases pursuant to a special Act;
  - it is necessary to keep the obligations and rights of the data controller responsible for processing in relation to employment;
  - the processing pursues political, philosophical, religious or trade-union aims and is carried out within the scope of legitimate activity of a civil association, foundation or other legal person of a non-profit nature;
  - it is necessary to the provision of sickness insurance, pension insurance (security), accident insurance, state social support and other state social



security benefits, social services, social care, assistance in material need, and the protection of children;

- the processing concerns personal data published by the data subject;
- the processing is necessary to secure and exercise legal claims;
- the processing relates exclusively to archival purposes pursuant to a special Act; or
- the processing is done in accordance with special Acts to regulate prevention, investigation, detection of criminal activities, prosecution of criminal offenses and the search for persons.

## 5. Data Transfer

5.1 If the controller carries out personal data processing for the purpose of offering business opportunities or services to the data subject, then certain conditions apply. With respect to transfer, a data controller may transfer to another data controller or data processor if the following conditions are met:

- the data was acquired in relation to activities of the data controller or the data in question consist of published personal data;
- the data is used exclusively for the purpose of offering business opportunities and services; and
- the data subject has been notified in advance of the transfer and it has not expressed disagreement with the transfer.

### 5.2 International Data Transfer

The transfer of personal data within the European Economic Area is not subject to additional requirements. Transfer to a country outside of the European Economic Area is only permitted:

- if the restriction on the free movement of personal data is prohibited by an international treaty ratified by the Parliament and binding for the Czech Republic (*e.g.*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108); or
- if the personal data are transferred on the basis of a decision of an institution of the European Union. In accordance with these decisions, transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

Notification to the Office is required in most circumstances.

5.3 Where either of the two conditions set out above are not met, the transfer of data outside of the European Economic Area is permitted with authorization from the Office and where the data controller proves that:

- the data transfer is carried out with the consent or by request of the data subject;
- sufficient specific guarantees of personal data protection have been created, *e.g.*, through contractual clauses;

- the personal data are part of publically accessible data files or accessible to someone who proves a legal interest on the basis of a special Act;
- the transfer is necessary to exercise an important public interest following from a special Act or from an international treaty binding the Czech Republic;
- the transfer is necessary for negotiating the conclusion of a contract in the interest of the data subject or 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 protection of rights and vital interests of the data subject.

5.4 The Office takes a number of circumstances into account in considering applications for authorization.

5.5 The Office has explained that it recommends consulting with the Office in reviewing whether a transfer comports with the US-EU Safe Harbor Framework. Also, it notes that a permit is not necessary for the use of the EU model contractual clauses; however, any deviation therefrom would require a permit.

See [www.uoou.cz/uoou.aspx?menu=41&submenu=44&lang=en](http://www.uoou.cz/uoou.aspx?menu=41&submenu=44&lang=en).

5.6 Special requirements may apply to the transfer of employee data.

See [www.uoou.cz/uoou.aspx?menu=41&submenu=46&lang=en](http://www.uoou.cz/uoou.aspx?menu=41&submenu=46&lang=en).

## 6. Data Security

Data controllers must have appropriate security measures in place to prevent unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transmission, other unauthorized processing, as well as other misuse of personal data. Data controllers and processors are required to document and develop these measures and perform risk assessments.

## 7. Breach Notification

Under the Act there is no requirement to notify the Office or the data subject in the event of a data breach. Data controllers should assess carefully whether to notify the Office, as voluntary notification can be taken into account when assessing the severity of fines.

## 8. Enforcement & Penalties

8.1 The Office may conduct inspections of data controllers. Data controllers are required to cooperate and assist in these inspections and a fine of up to CZK 25,000 may be imposed for the lack of cooperation.

8.2 If the inspector decides that a breach of the Act has occurred, it can determine what measures shall be adopted to remedy the breach and set a deadline for their adoption.

- 8.3 If a natural person commits an offense under the Act there are administrative fines ranging from CZK 100,000 to CZK 5,000,000. For legal persons or individuals in their business capacity, the fines range from CZK 1,000,000 to CZK 10,000,000.
- 8.4 The fines of CZK 5,000,000 for natural persons and CZK 10,000,000 for legal persons are reserved for breaches that affect a substantial number of people by interference in their private and personal life or that fail to fulfil obligations relating to personal sensitive data.
- 8.5 There are no criminal sanctions under the Act. However, “Unauthorised Use of Personal Data” is a criminal offense defined in the Penal Code. This offense can only be committed by natural persons and it carries a punishment of imprisonment of up to eight years.

## 1. Applicable Law

In Denmark, the EU Directive on Data Privacy has been implemented through the Act on Processing of Personal Data, Act No. 429 of May 31, 2000 (the “Act”). It covers data processing by public and private companies established in Denmark in connection with activities that take place in the EU. The Act also applies to data processed on equipment located in Denmark, though not to data that is merely transmitted through the country.

<http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/>

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Office for Personal Data Protection (the “DPA”)

2.2 **Registration.** Subject to certain exceptions found in § 49 of the Act, prior to the commencement of any processing of data carried out by or on behalf of a private data controller, the private data controller must notify the DPA. The registration should contain the following information:

- the name and address of the private data controller and of her representative, if any, and of 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 measures taken to ensure security of processing;
- the date of the commencement of the processing; and
- the date of erasure of the data.

## 3. Protected Personal Data

3.1 **Personal data** is any information relating to an identified or identifiable natural person.

3.2 **Sensitive personal data** is information concerning racial or ethnic background; political, religious or philosophical conviction; trade union membership; health, sexual or criminal matters; significant social problems; and other similar information related to one’s private life. Also covered in this definition are biological materials that can be used to identify an individual, such as blood and tissue samples.

## 4. Data Collection and Processing

4.1 When personal data is collected from the data subject, and unless an exception applies, the data controller must inform the data subject of the identity of the data controller, the purposes of the processing, and any further information necessary under the circumstances to enable the data subject to safeguard his or her interests, such as (i) the categories of recipients; (ii) whether responses are obligatory or voluntary, as well as possible consequence of failure to reply; and (iii) the rules on the right of access and the right to rectify data relating to the data subject

4.2 Data must be collected for specified, explicit, and legitimate purposes, and further processing must not be incompatible with these purposes. Further processing of data that takes place exclusively for historical, statistical or scientific purposes is not considered incompatible with the purposes for which the data were originally collected.

4.3 Personal data may only be processed if:

- the data subject has given her 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 data 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 data controller or in a third party to whom the data are disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

4.4 Special Considerations Regarding Sensitive Data

Generally, sensitive data cannot be processed unless:

- the data subject has given her 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 her consent;
- the processing relates to data which have been made public by the data subject; or
- the processing is necessary for the establishment, exercise or defense of legal claims.

Other specific exceptions include (i) where the processing is required by a public authority in the area of criminal law; (ii) where data is required for certain medical purposes by a health professional subject to the law on professional secrecy; and (iii) in the course of its legitimate activities by a foundation, association or other non-profit body with a political, philosophical, religious or trade union goal if the sensitive data relates to the members of the body or to persons who have regular contact with it in connection with its purposes. In addition, further requirements for data related to criminal offenses, serious social problems, identification numbers, and other private matters may apply.

## 5. Data Transfer

5.1 Where a data controller leaves the processing of data to a third-party processor, the data controller shall make sure that the processor is in a position to implement the technical and organizational security measures required by the Act and shall ensure compliance with those measures. The processing must be governed by a contract between the parties, which stipulates that the processor shall act only on instructions from the data controller and that the security provisions of the Act apply to the processor as well.

5.2 Disclosure to a third-party company for marketing purposes is generally not allowed unless the consumer has given explicit consent in accordance with the Danish Marketing Act, though there are some exceptions in which this may not apply.

### International Data Transfer

5.3 Additional requirements may be necessary for transfer to a third country. Transfer of data to a third country may take place if that country ensures an adequate level of protection.

5.4 Countries with adequate data protection include the European Economic Area (EEA), as well as those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

5.5 Additionally, data can be transferred to a third country if:

- the data subject has given her explicit consent;
- the 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;
- the transfer is necessary for the performance of a contract concluded in the interest of the data subject between the data controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject;

- the transfer is made from a register that according to law 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 offenses, 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 defense of the Realm, or national security.

5.6 The DPA may also authorize a transfer of personal data to a third country not deemed to have adequate data protection where the controller ensures adequate safeguards with respect to the protection of rights of the data subject. Specific conditions may be laid out for the transfer.

5.7 Personal data may be transferred to a third country not deemed to have adequate data protection without authorization from the DPA on the basis of contracts in accordance with the standard contractual clauses approved by the European Commission. In addition, the use of the binding corporate rules framework is approved.

See <http://www.datatilsynet.dk/english/third-countries/binding-corporate-rules-bcr/>.

## 6. Data Security

6.1 Data controllers and processors must implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or deterioration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in law.

6.2 More guidelines on the establishment of both technical and organizational security measures in connection with electronic data processing are laid down in Danish Standard DS 484, Standard for IT Security.

## 7. Breach Notification

The Act does not contain a provision requiring breach notification.

## 8. Other Considerations

8.1 Upon request, any individual has a right to have the data controller inform her of whether or not data relating to her are being processed. Where such data are being processed, communication to the individual shall take place in an intelligible form about:

- the data that are being processed;
- the purposes of the processing;
- the categories of recipients of the data; and

- any available information as to the source of such data.

8.2 A data subject may object to the processing of the subject's data, and if the objection is justified, the processing must cease.

## **9. Enforcement & Penalties**

9.1 Enforcement under the Act is accomplished through action by the DPA, which has the authority to supervise all data protection covered by the Act and issue injunctions if necessary.

9.2 A data controller is required to compensate data subjects for any damages that result from a violation of the Act. Additionally, unless other legislation provides a harsher penalty, violations of the Act are punishable by a fine or prison term of up to four months.



## 1. Applicable Law

In Finland, data privacy is governed by the Personal Data Act (523/1999). In 2000, the Personal Data Act was amended by the Act on the amendment of the Personal Data Act (986/2000) (the “Act”). The Act applies to the processing of personal data for anything, but purely personal purposes.

<http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf> (Unofficial English Translation)

<http://www.finlex.fi/fi/laki/ajantasa/1999/19990523>

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Data Protection Ombudsman and the Data Protection Board.

2.2 **Registration.** While Finland does not keep a registry of data processors, a data controller is required to notify the Data Protection Ombudsman of any automated data processing by sending a description of the file. There are also special notification requirements for certain transfers outside the EEA and for those engaged in credit data activity.

## 3. Protected Personal Data

3.1 Personal data means any information on a private individual and any information on his or her personal characteristics or personal circumstances, where these are identifiable as concerning her or members of her family or household.

3.2 Sensitive personal data means personal data that relates or is intended to relate to:

- racial or ethnic origin;
- social, political, religious affiliation or trade-union membership;
- 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.

## 4. Data Collection and Processing

4.1 When collecting personal data, the data controller or its representative must give the data subject information about the data controller, and, where necessary, information on the destination of the data and how the data subject can exercise his or her right in respect to processing of the data. If the data is collected in a manner other than directly from the data subject, the controller may not need to inform the data subject of the above information where doing so would be impossible or unreasonably difficult.

4.2 The purpose of the processing of personal data must be defined before collection occurs. Personal data cannot be processed in a manner inconsistent with the original defined purpose unless it is done for historical, scientific, or statistical reasons.

4.3 Personal data may only be processed if:

- the data subject has given her unambiguous 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 in order to protect the vital interests of the data subject;
- the processing is required by statute;
- there is a relevant connection between the data subject and the operations of the data controller, based on the data subject being a client or member of, or in the service of, the data controller or on a comparable relationship between the two;
- a company or other economic grouping processes data relating to its clients or employees;
- 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 data controller or a third party receiving the data; or
- the Data Protection Board has issued permission.

4.4 Special Considerations Regarding Sensitive Data

Generally, sensitive data cannot be processed. This prohibition does not apply to processing of:

- data where the data subject has given her explicit consent;
- data on the social, political or religious affiliation or trade-union membership of a person, where the person has himself/herself brought the data into the public domain;
- data necessary for the safeguarding of a vital interest of the data subject or someone else, if the data subject is incapable of giving her consent;
- data necessary for drafting or filing a lawsuit or for responding to or deciding of such a lawsuit;
- data in compliance with statute;
- data for the purpose of historical, scientific, or statistical research;
- member's data on religion, political, or social affiliation by an organization devoted to that purpose and where the data is not shared with a third party;
- membership data by a trade-union where the data relates to members or individuals with regular contact with the union and the data is not shared with a third party;
- data on trade-union membership, where necessary for the observation of the special rights and duties of the controller in the field of Labor Law;

- data collected in the course of the operations of a health care unit or a health care professional relating to the state of health, illness or handicap of the data subject or the treatment or other measures directed at the data subject, or other data, which are indispensable in the treatment of the data subject;
- data by an insurer during the course of its insurance activity where necessary for the determination of its liability to a policy holder or claimant; or
- data by a social welfare organization during the course of its operations where the data relates to the needs of the data subject or the benefits, support or other social welfare assistance received by the person.

## 5. Data Transfer

- 5.1 Data sharing is allowed. However, anyone who as an independent trader or business operates on the behalf of the data controller must, before starting the processing of data, provide the data controller with appropriate commitments and other adequate guarantees of the security of the data to the degree required of the data controller itself.
- 5.2 Transfer of data to a third country may take place if that country ensures an adequate level of protection. Additionally, data can be transferred to a third country if:
- the data subject has given his unambiguous consent;
  - the 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;
  - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
  - 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 or for special reasons, has been specifically provided in the Act;
  - the data controller, by means of contractual terms or otherwise, gives adequate guarantees of the protection of the privacy and the rights of individuals, or
  - the transfer is made using the EU model contractual clauses.
- 5.3 Countries with adequate data protection include all countries within the European Economic Area (EEA), as well as countries which the European Commission, pursuant to the EU Data Protection Directive 95/46/EC, has determined to guarantee an adequate level of protection. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

- 5.4 There is a special duty of notification with respect to transfers outside of the EEA. Notification to the Ombudsman is not required under most of the exceptions listed, including where there is consent. It is also not required where the European Commission has found there to be an adequate level of protection or where EU model contractual clauses are used.
- 5.5 The use of the EU model contractual clauses may also be used as the basis for the controllers own contractual clauses, but in this case they will be modified standard contractual clauses and the Ombudsman must be notified. In addition, the use of the binding corporate rules framework is authorized.

## **6. Data Security**

Data controllers must carry out the technical and organizational measures necessary for securing personal data against unauthorized access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing. The techniques available, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy are taken into account when determining which measures are necessary.

## **7. Breach Notification**

Finnish law does not require notification in the event of a breach. However, the Data Protection Ombudsman or Data Protection board has the authority to request certain actions in the event of a breach – including possible notification.

## **8. Other Considerations**

- 8.1 Upon request, any individual has a right to have the controller inform her of the contents or existence of a personal data file, the sources of the data, and the purpose of the personal data file relating to her. This right of access does not apply when:
- providing access to the data would compromise national security, defense or public order or security, or hinder the prevention or investigation of crime;
  - providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else;
  - the data in the file are used solely for historical or scientific research or statistical purposes; or
  - the personal data in the file are used in the carrying out of monitoring or inspection functions and not providing access to the information is indispensable in order to safeguard an important economic interest or financing position of Finland or the European Union.
- 8.2 A data controller is required, upon request of the data subject or on its own initiative, to rectify, erase, or supplement personal data files to ensure accuracy.
- 8.3 A data subject has the right to prohibit the data controller to process personal data for purposes of direct advertising, distance selling, other direct marketing, market research, opinion polls, public registers or genealogical research.

## 9. Enforcement & Penalties

- 9.1 Enforcement under the Act is accomplished through action by the Data Protection Ombudsman and the Data Protection Board.
- 9.2 At the request of the Data Protection Ombudsman, the Data Protection Board may:
- prohibit the processing of personal data, which does not comply with the 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 her interests or rights, provided that the file is not set up under a statutory scheme; and
  - revoke explicit permission to process data, if the processor no longer complies with the conditions set out in the original issuance of permission.
- 9.3 Violations of the Act may result in criminal liability resulting in fines or imprisonment of up to one year, as determined by Finnish Penal Code (38/1889). Additionally, a data controller may also be civilly liable to a data subject or another person for economic and other loss resulting from violations of the Act.

## 1. Applicable Law

Data Protection is regulated by the French Data Protection Act of January 6, 1978, which was thoroughly overhauled in 2004 by the Data Process Act (“DPA”), which implemented the EU Data Protection Directive. The data protection law does not apply to data processing carried out for the exercise of exclusively private activities.

<http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf> (English translation)

<http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/>

## 2. Data Protection Authority and Registration Requirements

- 2.1 The Commission Nationale de l’Informatique et des Libertés (the “CNIL”) is charged with overseeing compliance with the data protection law.
- 2.2 A data controller must notify the CNIL when it intends to process data, although there are some exceptions. Certain types of processing may require a declaration.
- 2.3 To summarize, the prior declaration requires, among other things:
  - purpose(s) of the processing;
  - identity and the address of the data controller;
  - possible interconnections between databases;
  - personal data processed and the categories of persons who may be concerned by the processing;
  - time period for which the data will be stored;
  - department or person(s) in charge of processing;
  - recipient(s) of the personal data; and
  - measures taken in order to ensure the security of the processing.
- 2.4 For the most common categories of processing of personal data, where violation of privacy or liberties is unlikely, the CNIL establishes and publishes standards intended to simplify the obligation to give notice of a processing to the CNIL. These standards specify the purposes of the processing covered by the simplified notification, the categories of personal data and the recipients to whom the personal data is disclosed.
- 2.5 Prior authorization from the CNIL is required for processing deemed potentially harmful to privacy and liberties, such as:
  - the processing of certain sensitive data categories;
  - transfer of data outside the EU to a country without adequate protection;
  - automated processing, which consists of a selection of people and is aimed at excluding some of them from the advantages of a right, a benefit or a contract;

- automated interconnection files; and
- biometric identity checks, for instance, for access controls.

2.6 The CNIL has two months to approve the application, and if it takes no action, the application is considered denied.

### 3. Protected Personal Data

3.1 **Personal data** is defined as 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 the individual.

3.2 **Sensitive personal data** is data directly or indirectly disclosing the data subject's racial or ethnic origins; political, philosophical or religious opinions; membership in a trade union; health or sexual life.

### 4. Data Collection and Processing

4.1 Parties must obtain data subjects' consent to collection and processing, although consent may be implied. There are some exceptions under Article 7 to the consent requirement. Sensitive data may only be collected with the data subject's express consent.

4.2 Data controllers must process personal data in compliance with the rules set out under Article 6 of the Data Processing Act, as follows:

- data must be collected and processed fairly and lawfully;
- data must be collected for a determined, explicit and legitimate purpose and must not be subsequently processed in a manner incompatible with this purpose;
- the collected data must be adequate, relevant and non-excessive regarding the purposes for which it was collected and subsequently processed;
- the data must be accurate, complete and up-to-date; and
- the data must be stored in a form that allows the identification of the data subjects for a period no longer than necessary for the purposes for which it was obtained and processed.

4.3 The processing of sensitive personal data is prohibited unless:

- the data subject has given consent;
- the processing is necessary to protect human life, and the data subject is unable to give consent due to legal incapacity or physical impossibility;
- the processing is specifically for an association that relates only to members of the association, and is not transmitted, unless consent is given for transmission;
- the personal data has been made public by the data subject;
- the processing is necessary for the establishment, exercise or defense of a legal claim;
- the process is necessary for health care;

- the process is for statistical purposes carried out by the National Institute of Statistics and Economic Studies or one of the statistical services of Ministries; or
- the processing is necessary for medical research.

## 5. Data Transfer

- 5.1 Data controllers may transfer data to parties in countries that are members of the EU and European Economic Area (EEA) to the same extent they could share information within France.
- 5.2 In order to share with other countries, the country must be recognized by the European Commission as providing an adequate level of protection in accordance with the 1995 European Data Directive 95/46/EC and the controller must notify the CNIL. Transfer to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.
- 5.3 A data controller cannot transfer personal data to any other country unless the data subject has given express consent or the situation meets certain other requirements for exemption, such as where the transfer is necessary for preserving the data subject's life.
- 5.4 The data controller can also apply to the CNIL for authorization to transfer to countries outside of the EU or European Economic Area where it has ensured an adequate level of protection by contract. The data controller may not begin transfer until it receives authorization from the CNIL. Here, the use of EU model contractual clauses or the binding corporate rules framework are relevant.
- See <http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/>.
- 5.5 In general, data cannot be processed by a third party unless they agree to follow the data controller's instructions, the third party processor offers adequate security, and the data controller and processor sign an agreement agreeing to the same.

## 6. Data Security

The data controller must take all necessary security precautions, with respect to the nature of the data and the risks caused by the processing to preserve the safety of the data, and notably to prevent them from being distorted, damaged, or accessed by non-authorized third parties.

## 7. Breach Notification

- 7.1 On May 28, 2012, the CNIL released new guidance for breach notification. The guidance pertains to a 2011 ordinance that came into force on April 1, 2012. Among other things, the ordinance amends existing French data protection law to reflect the EU e-Privacy Directive's (2009/136/EC) breach notification requirement for ISPs and others.
- 7.2 The Guidance provides that the ordinance applies to e-communication service providers including ISPs and mobile phone operators that are registered with the



French Authority for Regulation of Electronic Communications and Posts. It does not yet apply to online banks, e-commerce sites or other “information society” services.

- 7.3 It defines a violation under the ordinance, and in doing so states that malicious intent is but one possible scenario where the violation may occur. It also sets out examples of where a violation may occur, including: an intrusion into the customer database of an ISP, a confidential e-mail sent in error, and a mobile phone operator’s system making available to others the credit card information of subscribers that have ordered phones. According to the guidance, however, a computer virus on the personal computer of a user and not linked to the ISPs would not constitute a violation. Neither would the theft of a human resources database as it does not relate to the providing of the e-communication service to the public.
- 7.4 The guidance sets out a layered process for notification. First, where a violation occurs, regardless of its severity, CNIL must be notified without delay by letter setting out certain details of the breach. As far as notifying individuals, the company must assess the potential damage from the breach (considering, for example, theft or identify fraud or significant humiliation or damage to reputation) and whether it has applied the technological protection measures required, such as effective encryption, to determine whether to notify individuals in the first instance. Companies do not have to notify individuals where “adequate” measures have been taken. The guidance notes, however, that encryption is not effective where the key is stolen or otherwise compromised.
- 7.5 Second, CNIL will evaluate the breach and measures. If the breach is serious, CNIL can order a company to notify users and will do so within a month. CNIL has two months, however, to evaluate the corrective measures taken by a company. If CNIL does not respond, the company must immediately notify its subscribers regarding the breach. The guidance sets out the details that must be included in the notification to subscribers: the nature of the breach, contact details from whom to obtain additional information regarding the breach, and recommended measures to reduce the negative consequences of the breach. CNIL leaves the method of notification to individuals to the company so long as it can be verified.
- 7.6 Non-compliance with the ordinance can lead to fines of €300,000 and up to five years imprisonment, as well as CNIL sanctions.

## **8. Other Considerations**

If an organization has an appointed data protection officer (“DPO”), which is not mandated by law, an organization is exempt from making prior declarations to the CNIL. The appointment of a DPO does not, however, exempt an organization from requesting prior authorization, where necessary, *e.g.*, transfer of data to a country that does not have adequate protection to personal data.

## **9. Penalties**

- 9.1 The CNIL may issue a wide array of penalties including: (i) a warning; (ii) a formal demand; (iii) the issuing of an injunction to cease processing; (iv) financial sanctions of up to €150,000 for the first breach (and up to €300,000 in the case of a repeat breach within five years); and (v) the revocation of the CNIL's authorization.
- 9.2 Criminal sanctions may also be imposed of up to a maximum of five years' imprisonment and fines from €15,000 (and up to €75,000 for legal entities) to €300,000 (and up to €1,500,000 for legal entities).

## 1. Applicable Law

In Germany, data privacy is governed by laws at both the Federal and State level. The federal law and the main focus for businesses operating in Germany is the Data Protection Act (“Bundesdatenschutzgesetz,” or “BDSG”). The BDSG implements the EU Data Protection Directive and seeks to protect personal data processing by private organizations and the federal public authorities.

The BDSG applies where personal data is processed by a data controller established in Germany (and the processing occurs in the context of that establishment) or where the data controller is not established in the EU, but uses equipment situated in Germany to process personal data (other than for the purposes of transit).

The laws at the State level seek to protect personal data from being processed by State public authorities, and so tend to be of less practical importance to businesses.

[http://www.gesetze-im-internet.de/englisch\\_bdsq/federal\\_data\\_protection\\_act.pdf](http://www.gesetze-im-internet.de/englisch_bdsq/federal_data_protection_act.pdf)

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The principal authority under the BDSG is the Federal Commissioner for Data Protection and Freedom of Information. This position is established within the Federal Ministry of the Interior.

2.2 **Registration.** The BDSG requires all bodies that process personal data in an automated way to notify the relevant supervisory authority. However, in practice, this requirement is waived if a data protection officer has been appointed – a data protection officer becomes obligatory either where more than nine persons are regularly involved in automated data processing or where sensitive personal data is being processed. A data protection officer can be an employee or someone outside the organization with an understanding of data protection. When a data processor registers, they should provide the following information:

- name or title of the body;
- owners, managing boards, managing directors or other lawfully or constitutionally appointed managers and the persons placed in charge of data processing;
- address of the data controller;
- the business purposes of the body and of data processing;
- a description of the category or categories of data of the data subject and of the data or categories of data relating to the data subject;
- the recipients or categories of recipients to whom the data might be disclosed;
- standard data retention periods;
- plans to transfer data to third countries; and

- a general description allowing a preliminary assessment to be made of the appropriateness of the technical and organizational measures taken to ensure security of processing.

### 3. Protected Personal Data

- 3.1 **Personal data** is defined as any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).
- 3.2 **Sensitive personal data** is any information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

### 4. Data Collection

4.1 Personal data may be collected processed, and used if:

- necessary to create, execute or terminate legal obligation with the data subject;
- necessary to safeguard the legitimate interests of the data controller and where there is no reason to believe that the data subject has an overriding legitimate interest in ruling out the possibility of processing; or
- the personal data is available to the public or the data controller would be allowed to publish them, unless the data subject has a clear and overriding interest.

4.2 Sensitive data may only be collected where:

- allowed by law or urgently required for reasons of important public interest;
- the data subject has given consent;
- 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 her consent;
- the data involved are data which the data subject has manifestly made public;
- necessary to prevent a significant threat to the public security;
- it is urgently required to prevent significant disadvantages to the common good or to preserve significant concerns of the common good;
- it 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 the data are processed by health professionals or other persons subject to the obligation of professional secrecy;
- 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 and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort; or
- it is required for compelling reasons of defense or to fulfill supranational or intergovernmental obligations of a public body of the Federation in the

field of crisis management or conflict prevention or for humanitarian measures.

## **5. Data Processing**

- 5.1 Processing means the storage, modification, transfer, blocking, or deleting of personal data. Processing can only take place where explicitly permitted by the BDSG or where explicit consent of the data subject has been obtained in advance.
- 5.2 Where the data subject's consent has not been obtained, personal data can only be processed in the course of a business for its own commercial purposes if the processing is:
- necessary to create, execute or terminate legal obligation with the data subject;
  - necessary to safeguard the legitimate interests of the data controller and where there is no reason to believe that the data subject has an overriding legitimate interest in ruling out the possibility of processing; or
  - the personal data is available to the public or the data controller would be allowed to publish them, unless the data subject has a clear and overriding interest.
- 5.3 Sensitive personal data may only be processed where the data subject's consent has not been obtained 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 consent;
  - 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;
  - the data involved have manifestly been made public, by the data subject; 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.

## **6. Data Transfer**

- 6.1 A processor can only process personal data pursuant to the data controller's instructions.
- 6.2 The following, among others, must be specified in the contract between the processor and the data controller:
- the data subject and duration of the work required;
  - the type, extent and purpose of the processing of data, the type of data and category of data subjects;

- the rectification, deletion and blocking of data;
- the processor's obligations particularly with regards to any right to issue subcontracts;
- the data controller's rights over the processor and the processor's obligation to cooperate; and
- return of storage device and deletion of data.

### 6.3 International Data Transfer

Transferring data within a company group is, legally, no different than transferring data to an unrelated third party.

The transfer of personal data within the European Economic Area (EEA) is not subject to additional requirements (apart from the need for a legitimate reason). Transfer of data outside of the EEA cannot occur if the data subject has a legitimate interest in preventing the transfer, especially if the recipient does not ensure an adequate level of data protection.

An adequate level of data protection can be achieved by:

- transferring the data to a country that the European Commission has recognized as having adequate level of protection in accordance with the 1995 European Data Directive 95/46/EC;
- entering into binding corporate rules;
- entering into a data protection agreement based on the EU model clauses of the European Commission; or
- transferring the data to a US-based recipient who complies with the US-EU Safe Harbor Framework.

### 6.4 Where an adequate level of data protection cannot be ensured, a transfer can still be made if:

- the data subject has given consent;
- the transfer is necessary:
  - for the performance of a contract with the data subject;
  - for the performance of a contract, which has been or will be concluded in the interest of the data subject between the data controller and a third party; or
  - to protect the vital interests of the data subject;
- the transfer is legally required on important public interest grounds; or
- the transfer is made from a register, which is already publicly available.

## 7. Data Security

Data controllers must provide an adequate level of security against unlawful processing of personal data. The level of protection must be proportionate to the harm, which might result from such unlawful processing and must be appropriate to the nature of the data.

## **8. Breach Notification**

- 8.1 Under German law, companies are required to report any illegal transfer or illegal access to a data subject's:
- sensitive personal data;
  - personal data which are subject to professional confidentiality obligations;
  - personal data regarding criminal acts or administrative offenses; or
  - personal data regarding bank accounts or credit card accounts.
- 8.2 The breach notification requirement applies if the illegal access or transfer would lead to severe adverse effects on the rights or legitimate interests of the data subject.
- 8.3 Data subjects should be notified as soon as appropriate measures to safeguard the data have been implemented and notification would not endanger criminal prosecution.

## **9. Enforcement & Penalties**

Violation of German data protection laws are subject to fines of up to €300,000 or more per violation ("administrative offense"). The fine should exceed the financial benefit to the perpetrator derived from the administrative offense, and if that amount exceeds the statutory limits, then the limits may be disregarded. Where done wilfully or in exchange for a financial benefit ("criminal offense"), imprisonment of up to two years or an imposition of a fine is possible.

## 1. Applicable Law

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data is the main legislation applicable to the protection of personal data in Greece. This legislation implements EU Directive 95/46/EC and has been amended on subsequent occasions by further legislation (the "Data Protection Law").

[http://www.dpa.gr/portal/page?\\_pageid=33,43560&\\_dad=portal&\\_schema=PORTAL](http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL)

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** Hellenic Data Protection Authority (the "Data Protection Authority").

2.2 **Registration.** The data controller must notify the Data Protection Authority in writing of the creation and operation of a file or the commencement of processing. The notification must contain:

- the details of the data controller;
- address of all files and places where processing takes place;
- description of the purpose of the processing of personal data;
- the nature of the personal data;
- categories of data subjects;
- duration of processing;
- recipients or categories of recipients to whom personal data are announced or transferred; and
- any transfer and the purpose of such transfer of personal data to third countries.

## 3. Protected Personal Data

3.1 **Personal data** is information relating to the data subject. Information of a consolidated statistical nature not enabling the identification of data subjects is not considered as personal data.

3.2 **Sensitive personal data** is data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, social welfare and sexual life, criminal prosecution or convictions, as well as membership in related associations.

## 4. Data Collection and Processing

4.1 **Application.** The Data Protection Law applies where personal data is processed by a data controller or processor established in Greece, in a place where Greek law applies pursuant to public international law, and/or where the data controller is not established in the EU, but uses equipment situated in Greece to process personal data for purposes other than transit. The data controller is responsible for compliance with the Data Protection Law.



- 4.2 **Processing.** Processing of personal data is only permitted where the data subject has notice and has provided consent to such processing, except where processing is necessary:
- for the execution of a contract to which the data subject is party or for the adoption of measures further to the data subject's request during the pre-contractual stage;
  - for compliance with a legal obligation by the data controller;
  - in order to protect the vital interests of the data subject, if s/he is physically or legally incapable of giving her consent;
  - for the performance of a task carried out in the public interest or in the exercise of public function by a public authority or assigned by it to the data controller or a third party; or
  - for the purposes of a legitimate interest pursued by the data controller or a third party or third parties where such an interest prevails over rights and interests of data subjects and their fundamental freedoms are not affected.
- 4.3 **Notification.** Additionally, notification of the data subject is not necessary where processing:
- is carried out for purposes directly or indirectly related to an employment relationship or works contract or provision of services in the public sector and is necessary for the fulfillment of an obligation imposed by law or for the performance of obligations arising under these relationships where the data subject has been previously notified;
  - relates to clients or suppliers provided that data is not disclosed to third parties;
  - is administered by unions, companies, associations of persons and political parties and relates to personal data of their members or companies provided they have given their consent and the data is not transferred or disclosed to third parties;
  - involves medical data and is carried out by doctors or other persons providing medical services provided the data controller is bound by medical confidentiality or other professional/legal confidentiality and data is not disclosed to third parties;
  - is administered by lawyers, notaries public, fee-paid land registrars and court bailiffs and relates to the provision of legal services; provided the controller and its members are bound by a duty of confidentiality and the data is not transferred or disclosed to third parties; or
  - is carried out by the judicial authorities in the interests of justice.
- 4.4 **Sensitive Data.** Under the Data Protection Law, processing of sensitive data is prohibited, except with the prior approval of the Data Protection Authority. Such approval may be granted in the form of a license under specific circumstances, namely where:
- the data subject has consented in writing;

- processing is necessary to protect the vital interests of the data subject or third-party interest provided by law, if the data subject is incapable of giving her consent;
- processing relates to data published by the data subject or is necessary for the recognition, exercise or defense of a right in court or before a disciplinary body;
- processing relates to health matters and is carried out by a health professional under a duty of confidentiality where needed 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 national security, criminal or correctional policy and aids detection of offenses, criminal convictions or security measures, protection of public health or exercise of public control of fiscal or social services;
- processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained; or
- processing concerns data relating to public figures, provided that such data are in connection with a public office or the management of third-party interests and is carried out solely for journalistic purposes. The license is only granted where processing is absolutely necessary to ensure the right to information on matters of public interest, as well as literary expression and provided that the rights to privacy and family life are not infringed.

## 5. Data Transfer

- 5.1 Without further requirements being necessary, data transfer is permitted within the European Economic Area (EEA).
- 5.2 Outside the EEA, data transfer is permitted to countries that the Data Protection Authority has granted a license based on a finding that those countries' laws provide an adequate level of protection to personal data.
- 5.3 Countries with an adequate level of protection also include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.
- 5.4 A license is not required to transfer data to countries that the European Commission has deemed to have adequate levels of protection; however, transfer of data to such countries requires a transfer form be completed informing the Data Protection Authority of the transfer absent a license. The data controller should provide evidence of Safe Harbor certification where applicable.
- 5.5 Transfers outside the EU to a country that does not ensure an adequate level of protection will be allowed after a license has been granted by the Data Protection Authority provided that one or more conditions occur:
- the data subject has consented;
  - transfer is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent;

- transfer is necessary for the conclusion of a contract between the data subject and the data controller or between a third party and the data controller for the benefit of the data subject;
- transfer is necessary for the performance of pre-contractual measures at the request of the data subject;
- transfer is necessary to safeguard a superior public interest, especially the performance of a cooperation agreement with public authorities of another country where the data controller provides adequate safeguards for the protection of the data subject's privacy and rights;
- transfer is necessary for the establishment, exercise or defense of a right in court;
- transfer is made from a public register, which provides information to the public and is accessible by any member of the public who can demonstrate a legitimate interest; or
- where the data controller ensures that personal data and the rights of the data subject are adequately protected.

A license is not required where standard contractual clauses are in place, which would also need to be submitted and would be accepted provided there is no deviation from the standard terms. Although not included in the Data Protection Law, the Data Protection Authority also examines binding corporate rules for the purposes of approving intra-group transfers.

The Data Protection Law specifies that, if data processing is carried out on the data controller's behalf by a processor, there must be a written assignment. The assignment must provide in its terms that the processor will abide by the data controller's instructions as regards the data processing and will also comply with the confidentiality requirements.

## **6. Data Security**

Processing of data must be confidential and carried out by persons acting on instructions from the data controller or processor. The data controller is required to select persons with relevant professional qualifications, which provide adequate guarantees of technical knowledge and integrity. The data controller must additionally implement appropriate technical and organizational methods for the security of data in order to protect data from accidental or unlawful destruction or loss, alteration or unauthorized disclosure, and any other type of unlawful processing.

## **7. Breach Notification**

There are no requirements under the Data Protection Law requiring notification in the event of a breach; however, the Act for the Protection of Personal Data and Privacy (Law 3471/2006 Article 12) in the Electronic Communications Sector does have breach notification requirements that apply to providers of electronic communications.

## **8. Enforcement & Penalties**

- 8.1 The DPA may impose sanctions and penalties after an investigation undertaken either on its own initiative or pursuant to a complaint from another party.

- 8.2 If there is a breach of the data protection rules, the DPA may impose administrative sanctions on the data controller or any of its representatives. Such sanctions include:
- an order that the violation cease within a specified time limit;
  - fines ranging from approximately €1,000 – €140,000; and
  - in the event of more serious or repeated violations, a temporary or permanent revocation of the data controller or processor's license to process data and/or an order requiring the data controller to delete the data.
- 8.3 **Criminal sanctions** may apply for certain actions, including failure to notify the DPA that a file is being established, for failure to notify the DPA of any changes to the conditions of processing that formed the basis for the permit or for breach of the permit. Criminal penalties may also apply for unlawfully interfering with a personal data file, altering or affecting a personal data file in a harmful manner, or disclosing or making a personal data file accessible to unauthorized persons. Criminal penalties also apply to the unauthorized party who accepts or affects the personal data. Criminal sanctions may consist of imprisonment of up to three years and a financial penalty ranging from approximately €3,000 to €30,000.
- 8.4 **Civil liability** may result where a natural person or legal entity should have been aware that damage to another was likely. Civil recoveries could include an order of injunctive relief on behalf of the data subject, full compensation for damage to property and compensation for moral damages of at least €6,000 (unless a lesser amount is claimed).

## 1. Applicable Law

The Personal Data (Privacy) Ordinance (Cap. 486) (the “Ordinance”), first enacted in 1995 with significant amendments effective October 1, 2012, governs data protection in Hong Kong.

[http://www.legislation.gov.hk/blis\\_pdf.nsf/679916SD2FEE3FA94825755E0033E532/72DB9005F1984504482575EF000EBA7F/\\$FILE/CAP\\_486\\_c\\_b5.pdf](http://www.legislation.gov.hk/blis_pdf.nsf/679916SD2FEE3FA94825755E0033E532/72DB9005F1984504482575EF000EBA7F/$FILE/CAP_486_c_b5.pdf)

Revisions to the Ordinance took effect on April 1, 2013. These revisions require consent prior to the use of personal data in the context of targeted, direct advertising, and instruct individuals that, while direct marketers must notify individuals of their opt-out right prior to using personal data for the first time, individuals may choose to opt out at any time at no cost to the individual opting out. The Ordinance also provides for the following penalties: if “the transfer of personal data to third parties [is] for gain, the maximum penalty is a fine of HK\$1,000,000 and imprisonment for 5 years. For other direct marketing contraventions, the maximum penalty is a fine of HK\$500,000 and imprisonment for 3 years.”

On October 6, 2014, the Privacy Commissioner of Personal Data (discussed below) issued a Guidance Note on the Proper Handling of Customers’ Personal Data for the Banking Industry, clarifying the application of the Ordinance to banks as well as providing guidance regarding the collection and security of personal data associated with e-banking activities.

## 2. Data Protection Authority and Registration Requirements

- 2.1 The Ordinance established Hong Kong’s Office of the Privacy Commissioner for Personal Data (“OPCPD”), an independent statutory body established to oversee enforcement of the Ordinance, and provides for the appointment of a Privacy Commissioner for Personal Data (the “Commissioner”) who works in coordination with the Hong Kong Police.
- 2.2 The Commissioner may specify a class of “Data Users” that are required to submit “Data User Returns,” which will be maintained by the Commissioner in a register of data users that is open for public inspection. The specific information required of a class of data users is determined by the Commissioner and may differ from class to class.
- 2.3 “Data Users” required to submit “Data User Returns” may, upon written request from the Commissioner, be required to submit documentation or supply records verifying that the information they submitted in the Data User Return is accurate. Failure to respond to the Commissioner’s request is a punishable offense.
- 2.4 If a Data User’s situation changes after they submit a Data User Return, they are required to submit a “Change Order” detailing the changed circumstances such that the register can be updated to reflect the changes.

### 3. Protected Personal Data

- 3.1 “Personal Data” is defined as any representation of information in any document or in any form in which the information can be used or processed relating directly or indirectly to a living individual who can be identified from the data.

### 4. Data Collection and Processing

#### 4.1 Data Collection

Personal Data shall not be collected unless:

- the Personal Data is collected for a lawful purpose directly related to a function or activity of the Data User who is to use the Personal Data;
- the collection of Personal Data is necessary for and directly related to that purpose; and
- the Personal Data is adequate, but not excessive in relation to that purpose.

When collecting Personal Data directly from a data subject, the Data User must:

- inform the data subject as to whether the data subject is obligated to supply the Personal Data;
- inform the data subject on or before collecting the Personal Data as to the purpose for collecting the Personal Data and the classes of persons to whom the data may be transferred; and
- inform the data subject of his/her right to request and receive access to the data collected.

#### 4.2 Data Processing, Accuracy, and Retention

Data shall not be used for any purpose other than the Data User’s stated purpose for which the data was to be used at the time of collection.

Personal data may not be used in targeted, direct marketing without obtaining the data subject’s consent. In obtaining consent to use personal data in targeted, direct marketing, the Data User must inform the data subject of:

- The personal data that will be used; and
- That the data user may not use it without consent.

Regarding the accuracy of collected Personal Data, all practicable steps shall be taken:

- to ensure that the Personal Data collected is accurate while considering the purpose for which it is to be used; and
- to correct inaccuracies by notifying third parties as to inaccuracies and correcting or erasing inaccurate Personal Data in the possession of a Data Collector.

Personal Data shall not be retained longer than necessary to fulfil the purpose for which it was collected.

## **5. Data Transfer**

When Data Users notify data subjects of their purpose for collecting the Personal Data, they must include data transfers, both domestically and internationally, as a purpose for which they are collecting the data. A data subject may object to data transfer by requesting in writing that the Data Collector cease transferring the information or by submitting a complaint to the Commissioner.

### **5.1 International Data Transfer**

For Data Users who collect Personal Data in Hong Kong or whose principle place of business is in Hong Kong, transfer of Personal Data is prohibited unless:

- the place of transfer is specified in a notice to the data subject;
- the Data User has reason to believe a law with similar protections as provided by the Ordinance is in effect in the country;
- the data subject has consented in writing to the transfer;
- the user has reasonable grounds for believing the transfer of or the avoidance of an adverse action against the data subject, it's not practicable to obtain written consent, and data subject would most likely give consent; and
- the Data User has taken all reasonable precautions to ensure security.

Concerning the second requirement above, the Commissioner may publish a list of countries that have adequate protections in force. To date, the Commissioner has not published this list.

When Data Users notify data subjects of their purpose for collecting the Personal Data, they must include data sharing as a purpose for which they are collecting the data. A data subject may object to data sharing by requesting in writing that the Data Users cease sharing the information or by submitting a complaint to the Commissioner.

## **6. Data Security**

Rather than mandating specific security measures that must be adopted, the Ordinance contains general security principles to which a Data User must adhere. The Ordinance states that all practicable steps must be taken to ensure that Personal Data, including Personal Data held in an inaccessible form, held by a Data User is protected against unauthorized or accidental access, processing, erasure, or other use, having particular regard to:

- the kind of data and the harm that could result if any of those things should occur;
- the physical location where the data is stored;
- any security measures incorporated into any equipment in which the data is stored;
- any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and



- any measures taken for ensuring the secure transmission of the data.

Further, [2010 Privacy Commissioner Guidance](#) indicates that processors must take security measures “proportionate to the degree of sensitivity of the data and harm that will result from accidental or unauthorized access.” Actions which violate these principles may be actionable offenses punishable under the Ordinance and Hong Kong criminal law.

## **7. Breach Notification**

The Ordinance does not include a mandatory requirement to notify a data subject of a data security breach. The Commissioner, however, has issued recommended breach notification procedures for Data Users in the form of a “[Guidance Note](#).” First and foremost, the Guidance Note states that in the event of a breach a Data User should gather essential information related to the breach, such as when and how it occurred and/or was detected. The Guidance Note also recommends formation of a breach response team to coordinate all phases of breach response. After detecting the breach, the Guidance Note recommends contacting law enforcement agencies, regulators, and IT authorities to assist in containing the leak. Next, Data Users should evaluate the risk of harm presented to the Data Subjects by analyzing eleven factors listed in the Note. Upon a determination that risk of harm to Data Subjects exists, the Data User should notify all “relevant individuals.” The Guidance Note lists what should be included in the breach notification, including, for example, a summary of the risk of harm analysis, whether the incident has been reported to law enforcement, and a description of measures taken to prevent further loss. The notification should commence as soon as possible after detection of the breach. Although the provisions of the Guidance Note are not mandatory, failing to provide breach notification could be considered a violation of the Ordinance’s Data Security Principles, which is an actionable offense punishable by monetary penalties and, in some cases, criminal penalties.

## **8. Other Considerations**

### **8.1 Access to Personal Data**

8.2 The Ordinance permits a “Relevant Person,” defined as an individual who is a data subject and/or that individual’s legally authorized representative, to make a request to a Data User to be informed if the Data User collects information about the data subject, and, if the Data User has such data, to receive a copy of the data from the Data User. A Data User must respond to a data access request within 40 days of receipt. If the Data User has collected the data and a copy is requested, the Data User must provide the copy. The copy must be in the requested form, if practicable, and must be reasonably intelligible. If the data access request simply seeks to determine whether the Data User collects certain data, or if the Data User does not collect the data, a written explanation must be provided. If a Relevant Individual falsifies any information for the purpose of obtaining data or information about data to which they are not entitled, their actions are punishable offenses. A Data User must refuse to comply with a data access request if doing so violates other provisions of the Ordinance, and may refuse to comply with a data access request if it is not in writing, is duplicative, or does not include enough information for the Data User to determine what information to provide. Reasonable fees may be charged for access.

### **8.3 Correction of Personal Data**



- 8.4 If a Data User has supplied a copy of requested data pursuant to a data access request and the Relevant Individual determines that the data is inaccurate, the individual may submit a “data correction request.” A Data User must respond to a data correction request within 40 days. If a Data User determines that the data is in fact inaccurate, they must correct the data and supply a new copy. The Data User must also notify third parties who may have procured the data of the inaccuracy. If a Data User determines the data is accurate, they must provide a written explanation to the data correction requestor. Reasonable fees may be charged for corrections.

## **9. Enforcement & Penalties**

The Commissioner has full enforcement authority for the Ordinance. If the Commissioner learns of a breach of the Ordinance, via a complaint filed by a data subject or an independent investigation, the Data User can be served with an “Enforcement Notice” outlining the violation and requesting that remedial measures be taken immediately. Failure to comply with the Enforcement Notice is a criminal offense punishable by fines of HK\$1,000 per day for each day the violation continues and up to two years in prison. Repeat offenders may be fined HK\$2,000 per day and imprisoned for two years.

A Data User who provides the personal data of a data subject to another “for use by that other person in direct marketing” commits an offence and may be liable on conviction:

- If the data is provided for gain, to a fine of HK\$1,000,000 and to imprisonment for 5 years; or
- If the data is provided otherwise than for gain, to a fine of HK\$500,000 and to imprisonment for 3 years

## 1. Applicable Law

Act CXII of 2011 on Informational Self-determination and Freedom of Information (“Privacy Act”) implements EU Data Protection Directive 95/46/EC (the “Act”), which was enacted January 1, 2012. The Act applies to all data control and data processing activities undertaken in Hungary related to the data of individuals, data of public interest and data public on grounds of public interest.

[http://www.naih.hu/files/ActCXIIof2011\\_mod\\_lekt\\_2012\\_12\\_05.pdf](http://www.naih.hu/files/ActCXIIof2011_mod_lekt_2012_12_05.pdf)

<http://naih.hu/files/Infotv- MO.pdf>

The Act applies to both individuals and legal persons; it also applies to wholly or partially automatic and manual data control and data processing. The Act does not apply to natural persons processing data for purely personal purposes.

The provisions of the Act also apply if the data controller controlling personal data outside the territory of the European Union contracts with a data processor with a seat, business location, branch office or address or place of residence within the territory of Hungary to perform data processing, or uses equipment situated in Hungary, except if this device serves data traffic exclusively within the territory of the European Union. Such data controllers are obliged to designate a representative in Hungary.

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as “National Data Protection Authority”) enforces this Act. The National Data Protection Authority’s website (in Hungarian) is available at: <http://www.naih.hu/>.

2.2 **Registration.** Before initiating data processing activities the data controller must notify the National Data Protection Authority.

2.3 The notification is to include:

- purpose of data processing;
- legal basis of data processing;
- scope of data subjects;
- description of data relating to data subjects;
- source of data;
- duration of the data processing;
- type of transferred data, recipient of the transferred data and legal grounds for transfer, including cases of data transfer to third countries;
- name and address of the headquarters of the data controller and the technical data processor, the place of the data control and technical data processing, and the activity of the technical data processor related to data control;

- technical data processing method applied; and
- name and the contact information of the internal data protection officer in the event of taking part in the process.

2.4 No notification to the National Data Protection Authority is required where the data:

- processing activity relates to personal data of individuals associated with the data controller through employment, organizational membership, enrollment in educational institutions, or who are clients of the data controller (with the exception of the clients of financial organizations, public utility services and electronic telecommunications service providers);
- processing activity is carried out in accordance with the internal regulations of a church, a religious denomination or a religious community;
- processing activity relates to personal data concerning the disease or the state of health of a person receiving medical care for purposes of medical treatment, preservation of health or social welfare claims;
- processing activity relates to personal data registered with the aim of providing financial and other social support to the data subject;
- belongs to a media content provider;
- relates to scientific research which is not published; or
- relates to archived documents.

2.5 The National Data Protection Authority must register the data processing within eight days of receiving the notification; if this does not happen the data controller may commence processing.

2.6 In some cases this is extended to 40 days from receipt of notification where this relates to a financial institution or an electronic communication services provider processing additional data or the control of national official, labor or criminal data bases.

### 3. Protected Personal Data

3.1 **Personal Data.** Personal data is defined as that relating to the data subject, such as name and identification number of the data subject, as well as one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, as well as conclusions drawn from the data in regard to the data subject.

3.2 **Sensitive Personal Data.** Sensitive Personal Data or “Special Data” is defined as data concerning racial or national origin, political opinion or party membership, religious or other philosophical belief, membership in an interest representation organization, sex life, health, addiction, and criminal personal data.

- Criminal personal data is data relating to the data subject or a criminal record, generated in the course of or prior to the criminal proceedings, in connection with the crime or criminal proceedings, at the bodies

authorized to carry out criminal proceedings or to detect offenses, as well as at penal institutions.

#### **4. Data Collection and Processing**

- 4.1 Personal data may be processed if the data subject consents, or if it is provided for by law. Personal data processing may also be permitted where it is not possible to obtain the consent of the data subject and it is necessary to fulfill legal obligations applicable to the data controller or it is necessary to enforce the interests of the data controller or third party and that is proportionate with the restriction to the rights of the data subject.
- 4.2 If it is not possible due to incapacity to act or other circumstance beyond the data subject's control, his personal data may be processed where it is vital to protect his own or others vital interest, including dangers to the lives, physical integrity, or property of others.
- 4.3 Sensitive personal data may be processed if the data subject consents in writing, it is necessary to implement an international treaty, or is provided for by law to enforce basic rights ensured in the Fundamental Law, serves national security, prevents offenses, assists prosecution or is provided for by law for public interest purposes.
- 4.4 Sensitive personal data may also be processed where it is impossible to obtain the consent of the data subject or it would incur a disproportionate expense and:
  - it is necessary for the purpose of fulfilling the legal obligation of the data controller; or
  - it is necessary for the purpose of the legitimate interest of the data controller or a third party and the interest is proportional restrictive impact on the data subject's rights.
- 4.5 Furthermore, sensitive personal data may also be processed where the data subject is unable to give consent due to incapacity or other reason beyond his/her control and it is necessary to process the data to protect the data subject's vital interests or that of another person's.
- 4.6 The data controller defines the rights and obligations of the data processor concerning the processing of personal data with regard to the Act and relevant special legislation adopted in connection with the control of data. The data controller is responsible for the legitimacy of the issued instructions.
- 4.7 The data processor is not permitted to collaborate with other data processors during the course of the provision of their respective activities.
- 4.8 The data processor is not allowed to make any decision concerning the data collected. They can process the personal data they acquired knowledge of only in accordance with the instructions issued by the data controller. They are not allowed to process data for their own personal purposes and shall store and safeguard the personal data in compliance with the instructions issued by the data controller.

- 4.9 The contract concerning data processing must be finalized in writing. Any organization with vested interests in the use of the personal data to be processed for business purposes cannot be contracted to undertake data processing.

## **5. International Data Transfer**

- 5.1 Data transfers across borders are permitted where the data subject has provided explicit consent or there is compliance with the standards for data processing and an “adequate level” of protection in that country. A country will be deemed to have adequate levels of protection if:

- it is within the European Economic Area (EEA);
- there has been a legally binding Act from the European Union that the jurisdictions provide adequate protections for data;
- there has been an international treaty specifically containing the enforcement rights and remedies of data subjects;
- the use of standard contractual clauses between the parties such as those adopted by the European Commission (in such cases the data controller is obliged to notify the National Data Protection Authority of the use of the model clauses in order to register this fact, but no approval is needed); or
- the transfer is to a US recipient that has signed up to the US-EU Safe Harbor Framework (in these cases the National Data Protection Authority has to be notified by the data controller in order to register such transfer, but no approval is needed).

- 5.2 Personal data may also be transferred to another country in order to execute an international agreement to facilitate mutual legal assistance between authorities and for the avoidance of double taxation.

## **6. Data Security**

- 6.1 The data controller and the data processor are obliged to ensure data security within their respective scope of activities. The data must be particularly protected from unauthorized access, modification, transfer, disclosure, deletion or destruction, accidental destruction and damage, as well as failure of access due to changes of the technology applied. It is necessary to ensure that data stored in files cannot be directly connected and linked to the data subject.
- 6.2 When processing automated data the data controller and processor must ensure that unauthorized data entry is prevented; prevent the unauthorized use of data transfer devices; ensures the ability to control and determine which bodies of personal data have or can be sent using transfer devices; ensures the ability to restore the system should it malfunction; and report on errors that occur during automated processing.

## 7. Breach Notification

There is no general obligation to inform the National Data Protection Authority, but the designation of an internal data protection officer—who is entitled to ask the data controller or the data processor to terminate the unlawful data control—is mandatory.

## 8. Enforcement

8.1 Data subjects may request, and the National Data Authority may enforce:

- rectification of all incorrect personal data;
- ordering the blocking, deletion or destruction of illegally controlled personal data;
- prohibition of unlawful controlling or processing of personal data;
- prohibition of the transfer of personal data to foreign countries;
- ordering that a data subject be notified;
- imposing a fine of between HUF 100,000 to HUF 10,000,000; and
- informing the public of the decision of the National Data Protection Authority and the identity and actions of the data controller.

The National Data Protection Authority may take the data controller to court if he/she fails to comply with the order regarding public interest or public data for the purposes of public interest.

8.2 Criminal Sanctions:

If the Authority suspects that a crime has been committed they may initiate criminal proceedings at the appropriate court against the suspected person or entity.

The National Data Protection Authority, established in January 2012, has used its administrative powers to impose fines in several cases.

## 1. Applicable Law

India's Ministry of Communications and Information Technology ("Department of Information Technology") has implemented the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Privacy Rules"). Clarifications to the Privacy Rules were issued via Press Note by the Ministry. India's enabling legislation is India's Information Technology Act 2000 (the "Act"). While India continues to adhere to the Information Technology (Reasonable Security Practices and [Procedures and Sensitive Personal Data or Information\) Rules, 2011](#) (Rules) enacted in 2011, the Centre for Internet and Society presented a new Privacy (Protection) Bill, [2013 \(Bill\), on September 30, 2013](#). The Bill seeks to further refine provisions of the Rules, with a focus on protection of personal data through limitations on use and requirements for notice. The collection of personal data would be prohibited unless "necessary for the achievement of a purpose of the person seeking its collection," and, subject to sections 6 and 7 of the Bill, "no personal data may be collected under this Act prior to the data subject being given notice, in such form and manner as may be prescribed, of the collection." The Bill acknowledges the collection of data with and without consent; the regulation of personal data storage, processing, transfer, and security; and discusses the different types of disclosure.

[http://deity.gov.in/sites/upload\\_files/dit/files/GSR313E\\_10511\(1\).pdf](http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf)

<http://pib.nic.in/newsite/erelease.aspx?relid=74990>

<http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan010239.pdf>

## 2. Data Protection Authority and Registration Requirements

- 2.1 No specific data protection authority exists, but the Privacy Rules state that in the case of a breach, a "Body Corporate," as defined under the Act, must answer to "the agency mandated under the law" (presumably, the Ministry).
- 2.2 There are no registration requirements for the collection of data. However, the Data Security Council of India (the "DSCI") provides a certification service by which organizations within India may become "DSCI Privacy Certified."

## 3. Protected Personal Data

- 3.1 **Personal information** is defined as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a corporate entity, is capable of identifying such person.
- 3.2 **Sensitive personal data or information** is defined as "personal information" which consists of information relating to any of the following: passwords; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; any detail relating to any of the above as provided to a corporate entity for providing service; and

any of the information received under the above by a corporate entity for processing, stored or processed under lawful contract or otherwise. Data or information is not sensitive and personal if it is available in the public domain or furnished under the Right to Information Act of 2005.

#### **4. Data Collection and Processing**

4.1 The Privacy Rules apply to data collection, but do not define processing.

4.2 The Privacy Rules requires a Body Corporate<sup>5</sup> that collects, receives, possesses, stores, deals, or handles sensitive or personal data to provide a privacy policy for handling of such data and ensure that the policies are available for view by the data subjects who have provided the information under contract. The policy shall provide for:

- clear and easily accessible statements of its practices and policies;
- the type of personal or sensitive personal data or information collected;
- the purpose of collection and usage of such information;
- the disclosure of information including sensitive personal data or information; and
- reasonable security practices and procedures.

4.3 Data may be collected and processed when all of the following conditions are met:

- the data subject has provided written consent and is aware at the time of collection that the information is being collected, the purpose of collection, the intended recipients of the information; and the name and address of the agency that is collecting and will retain the information;
- the data subject has been provided with the option not to provide its sensitive personal data or information;
- the data subject is permitted to withdraw his/her consent, in writing, at any time;
- the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
- the collection of the sensitive personal data or information is considered necessary for that lawful purpose.

#### **5. Data Transfer**

5.1 Disclosure of data to a third party requires prior permission of the data subject, whether the information is provided under contract or otherwise, except in the following situations:

- the disclosure has already been agreed to in a contract;
- the disclosure is necessary for compliance with a legal obligation;
- the data is shared with government agencies with the authority to obtain the data for the purpose of verification of identity, or for the prevention,

---

<sup>5</sup> A Body Corporate is a corporate entity as defined under the Act, See § 2(c) of the Privacy Rules.



- detection, investigation, prosecution, and punishment of offenses, including cyber incidents; or
- the disclosure is pursuant to an order under the law.

5.2 Data may be transferred domestically or internationally to any person or Body Corporate that ensures the same level of data protection that is adhered to by the Body corporate, but the transfer is allowed only if:

- the data subject consents; or
- the transfer is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and the data subject.

## **6. Data Security**

6.1 A Body Corporate is required to implement reasonable security practices and procedures. The Privacy Rules indicate that reasonable practice methodologies include IS/ISO/EIC 27001 or other measures that have been pre-approved by the central government and are subject to annual audits by a central government-approved auditor.

## **7. Breach Notification**

7.1 There is no mandatory requirement to report data security breach incidents under the Privacy Rules.

## **8. Other Considerations**

8.1 Data retention rules state that information should not be retained longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law.

8.2 A clarification to the Privacy Rules stating that a “Body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is exempt from the requirement to obtain consent” was issued via Press Note by the Department of Information and Technology. Accordingly, outsourcing service providers in India should be exempt from obtaining consent from the individuals whose data they process.

## **9. Enforcement & Penalties**

9.1 A corporate entity may be liable for up to Rs. 50,000,000 for the negligent failure to implement and maintain reasonable practices and procedures, causing wrongful loss or gain.

## 1. Applicable Law

In Indonesia there is no comprehensive data protection law. There are however several laws that concern data privacy;

Indonesian Constitution

Article 28G of the Indonesian Constitution provides some protection that has been said to form the basis of a privacy right:

“Every person shall have the right to the protection of his/herself, family, honour, dignity, and property and shall have the right to feel secure and receive protection from the threat of fear to do or not do something that is a human right.”

[http://www.ilo.org/wcmsp5/groups/public/---ed\\_protect/---protrav/---ilo\\_aids/documents/legaldocument/wcms\\_174556.pdf](http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_174556.pdf)

The Law on Information and Electronic Transaction (2008) (“IET Law”)

The IET Law sets out a wide range of electronic transaction provisions. It covers areas concerning the use of electronic signatures in contracts to prohibited defamatory content in electronic communications. Relating to privacy law, the IET contains a provision (Article 26) that prohibits the use of any personal data through electronic media without the consent of that person. However, there is little guidance provided on the implications and enforcement of this broad prohibition. In October of 2012, Indonesia issued its first regulation under the IET, Government Regulation No. 82 of 2012 Concerning Electronic System and Transaction Operation (“Regulation 82”). Companies have until 2017 to comply with its requirements.<sup>6</sup>

The language of the regulation is available here: [http://rulebook-jica.ekon.go.id/indonesia/4902\\_PP\\_82\\_2012\\_i.html](http://rulebook-jica.ekon.go.id/indonesia/4902_PP_82_2012_i.html).

An English translation is available here: [http://rulebook-jica.ekon.go.id/english/4902\\_PP\\_82\\_2012\\_e.html](http://rulebook-jica.ekon.go.id/english/4902_PP_82_2012_e.html). This regulation makes a distinction between Electronic Systems Providers who perform “public services” and those which perform “non-public services,” although these terms are not defined.

Indonesian Human Rights Law

Article 32 of Indonesian Human Rights 39 of 1999 provides some recognition of the right to privacy as a human right.

<http://www.asiapacificforum.net/members/full-members/indonesia/downloads/legal-framework/indonesiaact.pdf> (Unofficial English Translation)

---

<sup>6</sup> [http://rulebook-jica.ekon.go.id/english/4902\\_PP\\_82\\_2012\\_e.html](http://rulebook-jica.ekon.go.id/english/4902_PP_82_2012_e.html)

## Health Law

Article 57 of Law 36 of 2009 guarantees that all Indonesian citizens have a right to privacy in their health information. There are exceptions to this rule when disclosure is:

- Commanded by Law
- Commanded by a court order
- In the public interest
- In the interest of the person

Applicable law in original Indonesian can be found here<sup>7</sup>;

<http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/91185/105616/F-1979234557/IDN91185%20IDN.pdf> (Unofficial English Translation)

## Banking Law

Indonesian Banking law also provides some privacy protections against the unlawful use or disclosure or confidential information. This includes criminal penalties for those who disclose.

An unofficial English translation of Act no. 7 of 1992 as amended by Act. No. 10 of 1998 (“Banking Law”) can be found here: <http://www.bu.edu/bucflp/files/2012/01/Act-No.-7-of-1992-Concerning-Banking.pdf> (Unofficial Translation).

Indonesia’s Financial Services Authority further issued Regulation No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector (“Consumer Protection Regulation”) on August 6, 2013, seeking to [encourage the growth of the financial service industry while still protecting its consumers](#).

An unofficial comparison between the Indonesian Original and English Translation of Regulation No. 1/POJK.07/2013 can be found here: <http://www.scribd.com/doc/171351025/Perojk-No-1-POJK-07-2013-Indonesia-Financial-Consumer-Protection-Wishnu-Basuki#scribd>

## **2. Data Protection Authority and Registration Requirements**

- 2.1 There is no general data protection authority in Indonesia.
- 2.2 Regulation 82 requires Electronic System Providers which provide public services to register with the Ministry of Communication and Information Technology. Electronic System Providers which provide non-public services may register, but are not required to do so.

## **3. Protected Personal Data**

- 3.1 There is no universal definition of personal data under current Indonesian law. Regulation 82 defines personal data broadly as any information which is specific to an individual and is treated and stored as confidential.

---

<sup>7</sup> For purposes of translation and due to a lack of availability of English text Google Translate was used to translate portions of this document.

#### **4. Data Collection and Processing**

4.1 When collecting Personal Data, Regulation 82 requires Electronic Systems Providers to:

- maintain the confidentiality;
- obtain consent before collecting, unless otherwise provided by regulations; and

#### **5. Data Sharing**

5.1 Regulation 82 requires Electronic Systems Providers to use Personal Data only in accordance with the purpose for which consent for collection was obtained.

#### **6. Data Security**

6.1 Regulation 82 requires Electronic Systems Providers to have an information security agreement, management policy and audit mechanisms.

#### **7. Breach Notification**

7.1 In case of breach, Regulation 81 requires Electronic Systems Providers to notify the owner of the Personal Data in writing. If the breach is a serious breach caused by a third party, the Electronic System Operator must secure the data and immediately report the breach to law enforcement or a regulatory agency.

#### **8. Enforcement & Penalties**

8.1 Under Article 47 of the Banking Law, revealing personal data may result in imprisonment of two to four years and a fine of between 4 and 8 billion Indonesian Rupiah.

8.2 Certain enumerated sections of Regulation 82 provides for administrative sanctions, which may be in the form of a written warning, an administrative fee, a temporary suspension, or removal from the registry. Regulation 82 makes clear that these sanctions do not replace criminal and civil liability. The exact penalties are to be the subject of future regulations.

## 1. Applicable Law

In Ireland, data privacy is governed by the Data Protection Act 1988 (the “Act”), available at <http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html>.

The Act was amended in 2003 by the Data Protection (Amendment) Act 2003, available at <http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html>.

The Act applies where personal data is processed by a data controller established in Ireland (and the processing occurs in the context of that establishment) or where the data controller is not established in Ireland, but uses equipment situated in Ireland to process personal data (other than for the purposes of transit).

The Act does not apply where the data was at any time kept for the purpose of safeguarding Ireland’s security, where the data consists of information that is required by law to be available to the public, or the data is kept by an individual for his personal/household affairs.

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** Office of the Data Protection Commissioner.

2.2 **Registration.** Data controllers and processors must register with the Office of the Data Protection Commissioner if they have (i) a legal presence in or use equipment in Ireland and (ii) hold personal data in an automated form.

2.3 All data controllers and processors must register unless:

- the data controller is a body that is not established or conducted for profit;
- the sole purpose of the processing is the keeping in accordance with law of a public register;
- the data controller only processes manual data;
- they are processing data relating to customers and suppliers;
- they are processing data relating to personnel administration;
- the data is processed by candidates who are holders of elective political office, which is carried out for the purpose of providing advice or assistance to electors;
- they are educational institutions processing data relating to the provision of educational services;
- they are legal professionals processing data for professional purposes;
- they are companies that are processing data in relation to shareholders, directors or other offers for compliance under the Companies Acts 1963-2012; or
- data is processed with a view to the publication of journalistic, literary or artistic material.

2.4 Registration is mandatory and can never be exempted for the following entities:

- Insurance undertakings (not including brokers);
- financial institutions;
- credit institutions;
- data controllers whose business consists of direct marketing;
- data controllers whose business consists of providing credit references;
- data controllers whose business consists of collecting debts;
- Internet access providers;
- telecommunications network or service providers;
- data controllers that process genetic data within the meaning of section 41 of the Disability Act 2005;
- health professionals processing personal data related to mental or physical health; and
- data controllers whose business consists of processing personal data for the supply of others (when not for journalistic, literary or artistic purposes).

### 3. Protected Personal Data

3.1 **Personal data** is defined as data relating to a living individual who is or can be identified either from the data or from the data in conjunction with the other information that is in, or is likely to come into, the possession of the data controller.

3.2 **Sensitive personal data** is defined as personal data regarding:

- the racial or ethnic origin, the political opinions, or the religious or philosophical beliefs of the data subject;
- membership in a trade union;
- the physical or mental health or condition or sexual life of the data subject; or
- any proceedings for an offense 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.

### 4. Data Collection and Processing

4.1 In the absence of consent from the data subject, personal data may only be processed where processing is necessary for:

- the performance of a contract to which the data subject is a party (including pre-contractual measures requested by the data subject);
- compliance with a legal obligation;
- preventing injury or other damage to the health, or serious loss or damage to the property, of the data subject;
- the administration of justice;
- the performance of a function conferred on a person by statute;
- the performance of a government function;
- protecting the vital interests of the data subject where seeking consent of the data subject is likely to result in those interests being damaged; or

- the purpose of the legitimate interests pursued by a data controller, except if processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

4.2 Sensitive data may only be processed where the requirements for processing personal data have been met and the:

- data subject has given explicit consent;
- processing is necessary for the purpose of exercising or performing any right or obligation, which is conferred or imposed by law on the data controller in connection with employment; r
- processing is necessary to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be reasonably obtained;
- processing is carried out in the course of its legitimate activities by a "not-for-profit" organization in respect of its members or other persons in regular contact with the organization;
- processing is carried out in the course of its legitimate activities by an organization that exists for political, philosophical, religious or trade-union purposes in respect of its members or other persons in regular contact with the organization;
- processing involves information that has been published by the data subject;
- processing is necessary for the administration of justice, for the performance of a duty conferred by statute, or for performance of a government function;
- processing is necessary for obtaining legal advice, obtaining information in connection with legal proceedings, or where processing is necessary for the purposes of establishing, exercising or defending legal rights;
- processing is necessary for obtaining data for medical purposes;
- processing is by a political party or candidate for election in the context of an election;
- processing is for assessing or paying a tax liability; or
- processing is for administering a social welfare scheme.

## 5. Data Transfer

5.1 A data processor is only entitled to process personal data to the extent and under conditions agreed upon with the data controller in a written contract or written authorization. The data controller must take reasonable steps to ensure that the data processor complies with the contract. The contract should set out:

- the conditions under which the data may be processed; and
- the security measures the data processor must implement.

## 5.2 International Data Transfer

The transfer of personal data within the European Economic Area is not subject to additional requirements. Transfer to a country outside of the European Economic Area is prohibited unless that country has an adequate level of protection for the privacy and rights of the data subject.

5.3 Countries with an adequate level of protection include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/35/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

5.4 Where an adequate level of data protection cannot be ensured in the destination country, a transfer can still be made where it is:

- required/authorized by law;
- necessary for performing contractual obligations either between the data controller and the data subject or at the request of the data subject;
- necessary in regards of substantial public interest;
- for the purpose of obtaining legal advice;
- preventing injury or other damage to the data subject's health or to prevent serious loss to the property of the data subject;
- an extract from a statutory public register;
- authorized by the Office of the Data Protection Commissioner; or
- consented to by the data subject.

5.5 The incorporation of EU Model Clauses into the data transfer contract will ensure adequate levels of protection and thus will be permitted. This can also be achieved through the use of binding corporate rules (whereby multinational companies draft and submit these guidelines to the Office of the Data Protection Commissioner for approval—these internal rules then apply to cross border transfers of data).

## 6. Data Security

Data controllers must have appropriate security measures in place taking into account technological development and the cost of implementing the measures. These measures must provide a level of security appropriate to (i) the harm that might result from unauthorized or unlawful processing, accidental or unlawful destruction or loss of data; and (ii) the type of data processed.

## 7. Breach Notification

The Office of the Data Protection Commissioner has published a non-binding Code of Practice regarding breach notification. This suggests notifying the data subject of the breach based on the type and degree of breach. If caused by a data processor, the data controller should be notified. Moreover, all incidents should be reported to the Office of the Data Protection Commissioner as soon as the data controller is made aware of the incident, unless the breach affects under 100 data subjects; the affected data subjects have been told without delay; or where the breach does not involve sensitive personal data or personal data of a financial nature.



The guidelines also set out how the Office of the Data Protection Commissioner may deal with the breach.

These do not apply to providers of publicly available electronic communications services in public communications networks in Ireland, as they have mandatory breach notification obligations covered by the EU e-Privacy Regulations.

## **8. Enforcement & Penalties**

- 8.1 The Data Protection Commissioner may investigate whether the provisions of the Act have been breached or are likely to be breached.
- 8.2 The Data Protection Commissioner has the power to issue:
- Information Notices requiring any person to provide the Data Protection Commissioner with whatever information he/she needs to carry out his/her functions, such as to pursue an investigation;
  - Enforcement Notices requiring a data controller or data processor to take whatever steps the Data Protection Commissioner considers appropriate to comply with the terms of the Act; and
  - Prohibition Notices under which the Data Protection Commissioner may prohibit the transfer of personal data from the State to a place outside the State.
- 8.3 The Act provides for criminal penalties in the following amounts:
- the Data Protection Commissioner may institute summary proceedings for a violation of the Act. The penalty for a conviction in such a proceeding cannot exceed €3,000; and
  - convictions resulting from an indictment for a violation of the Act carry a maximum penalty of €100,000.
- 8.4 Data processors and data controllers who fail to meet their data protection obligations can also be civilly liable to individuals who have been injured as a result of that failure.

## 1. Applicable Law

In Italy, data protection is primarily regulated by Legislative Decree of 30 June 2003 no. 196 (the “Code”), which implemented Directive 95/46/EC on data protection (“Data Protection Directive”) and Directive 2002/58/EC on the protection of privacy in the electronic communications sector (“Privacy and Electronic Communications Directive”). The Code became effective on January 1, 2004.

[http://www.garanteprivacy.it/web/guest/home\\_en/italian-legislation](http://www.garanteprivacy.it/web/guest/home_en/italian-legislation)

The Code applies to data controllers that are natural or legal persons, public authorities, associations or other agencies which alone or jointly with another data controller determine the purposes and means of processing personal data, including security matters. Jurisdiction is established on the basis of data processing taking place in Italy or using means of processing established in Italy.

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Italian Data Protection Authority (“DPA”), or the “Garante per la protezione dei dati personali,” can be found at [http://www.garanteprivacy.it/web/guest/home\\_en](http://www.garanteprivacy.it/web/guest/home_en). The DPA enforces the Code and maintains the register of notification.

2.2 **Registration.** The data controller must notify the DPA of the processing of personal data if the processing involves:

- genetic data, biometric data, or other data disclosing geographic location of individuals or devices by means of an electronic communications network;
- data disclosing health and sexual orientation and activity where processed for specified health-related reasons;
- data disclosing sexual orientation and activity or psychological profile(s) where processed by not-for-profit associations, bodies or organizations that have a political, philosophical, religious or trade-union character;
- data processed using electronic means aimed at profiling the data subject and/or his personality, analyzing consumption habits or choices, or monitoring use of electronic communications services, except for such processing operations that are technically indispensable to deliver electronic communications services to users;
- sensitive data stored in databases for recruitment services on behalf of third parties, or used for opinion polls, market surveys and other sample-based surveys; or
- data stored in databases operated electronically in connection with creditworthiness, assets and liabilities, proper performance of obligations, and unlawful and/or fraudulent activity.

### 3. Protected Personal Data

- 3.1 **Personal Data.** According to Section 4 of the Code, “personal data” is any information relating to natural persons who are or can be identified, even indirectly, by reference to any other information including a personal identification number. The Code recognizes sub-categories of personal data, including traffic and location data, sensitive data and judicial data.
- 3.2 **Sensitive Personal Data.** This means personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade union character, as well as personal data disclosing health and sex life.

### 4. Data Collection and Processing Requirements

- 4.1 Express consent is required to process data by private bodies or profit-seeking public bodies. Such consent is deemed to be effective if it is freely given, is specific 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 as required by the Code (*i.e.*, according to the “informed consent” principle).
- 4.2 However, consent is not required if the processing of personal data, in most instances with the exclusion of any circulation thereof (and where it is not sensitive data):
- is necessary to comply with an obligation imposed by law;
  - is necessary for the performance of obligations under a contract to which the data subject is a party (or to comply with requests made by the data subject prior to entering into a contract);
  - relates to data taken from publicly-available registers or records;
  - relates to data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy (*e.g.*, data derived from statements of accounts, data from Companies’ Register or Chamber of Commerce including details of shareholders, registered and operational addresses, etc.);
  - is necessary to protect life or physical safety;
  - is necessary for defending a legal claim and related activities (specific exception is provided for private investigation reports due to be used as means of evidence in judiciary proceedings);
  - is necessary to pursue a legitimate interest of either the data controller or a third-party recipient in the cases specified by the Italian DPA, without prejudice to any prevailing legitimate interest of the data subject;
  - certain internal communications within and between not-for-profit associations, bodies or organizations, and where relating to purposes in their constitutional documents;
  - is necessary for scientific and statistical purposes in compliance with any relevant codes of practice (which are listed in Annex A of the Code), or for certain historical archive purposes;

- is necessary to process CVs for recruitment purposes, provided that the data subject sends the CV voluntarily and the data controller provides the appropriate notices; or
- relates to data dissemination within controlled or affiliated companies, for administrative or accounting purposes.

4.3 Sensitive data may only be processed with both the data subjects' written consent and the DPA's prior authorization (there are some general authorizations issued by the DPA, so specific clearance is not always required). Data controllers do not need consent or DPA authorization where:

- the data concerns members of religious organizations recognized under Italian law and where the data are used exclusively for religious purposes, and are not disclosed externally;
- the data concerns members of trade unions and/or relations between trade associations or organizations to other trade unions and/or trade associations, organizations or confederations; or
- it is necessary to process CVs for recruitment purposes, provided that the data subject sends the CV voluntarily and the data controller provides the appropriate notices.

4.4 Sensitive data may also be processed without consent, provided the DPA's authorization is sought:

- where it involves certain internal communications within not-for-profit associations, bodies or organizations, and where it relates to purposes in their constitutional documents (subject to restrictions, including no external disclosure and prior notice to the data subjects), provided certain conditions are met;
- if the processing is necessary to protect life or physical safety;
- if it is necessary for defending a legal claim and related activities (subject to specific restrictions); and
- if the processing is necessary to comply with employment or health and safety law or relates to social security provisions.

4.5 Data disclosing health information may not be disseminated.

4.6 It is noteworthy that the Code contains specific provisions with respect to judicial data and with respect to data processing by specific sectors, such as healthcare, education, banking, electronics communication services, journalism, non-profit public bodies and more.

## 5. Data Sharing

5.1 In order for a third party to process data on behalf of the data controller, he or she must be appointed either as a data processor or as a person in charge of the processing. Data processors or the person in charge of processing must be selected in view of their experience, capabilities and reliability.

- 5.2 Written and specific instructions must be provided to both the data processors and persons in charge of processing, either through a specific letter of appointment or by contractual provisions.
- 5.3 The data processor shall abide by the instructions given by the data controller in carrying out the processing. The data controller shall ensure complete compliance with these instructions and with compliance with the data controller's instructions by performing regular controls.

## **6. International Data Transfer**

- 6.1 Without further requirements being necessary, data controllers may transfer personal data among the EU Member States and the European Economic Area. Such transfer can only be prohibited when it is made for the purposes of avoiding the provisions of the Code, although the DPA has never exercised this power thus far.
- 6.2 Personal data may be transferred to countries outside the European Economic Area:
- if the data subject has given her consent either expressly or, where the transfer concerns sensitive data, in writing;
  - where the transfer is authorized by the Italian DPA on the basis of adequate contractual safeguards (typically, EU model clauses), or binding corporate rules where the transfer is within the same group of companies; the Italian DPA must, however, approve of any BCR filed with any foreign lead authority through a specific procedure;
  - where the transfer is based on the EU standard model clauses, which are the object of a general authorization needing no further filing or approval;
  - where the transfer is to organizations in the United States that have been certified to the US-EU Safe Harbor Framework;
  - where the transfer is to a country deemed to provide adequate protection for personal data by a decision of the EU Commission;
  - 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 under the Code or Italian law or more widely and where the transfer concerns sensitive or judicial data;
  - if the transfer is necessary to protect life or physical safety;
  - if the transfer is necessary for defending a legal claim and related activities (subject to specific restrictions);
  - if the transfer is carried out in response to a request for access to information in a public records (subject to specific restrictions); or
  - is necessary for scientific and statistical purposes in compliance with any relevant codes of practice (which are listed in Annex A of the Code), or for certain historical archive purposes.

- 6.3 The Italian DPA does not need to authorize independent transfers outside of the EU where the EU model clauses, US-EU Safe Harbor Framework or approved binding corporate rules are used, but the DPA retains the right to request a copy of the relevant agreement. It may be necessary to file the model clauses used where the data transfer will be to a data processor operating outside the EU and/or to notify the Italian DPA where a sub-processor is used.

## **7. Security**

- 7.1 Data controllers must take suitable preventative security measures so as to minimize the risk of destruction, loss and unauthorized access. In assessing what measures are suitable, the data controller should take into account current technological innovations and the nature and any specific features of the processing.
- 7.2 The Code refers to specific security measures required where processing of personal data is carried by electronic means (the measures are further specified in Annex B of the Code):
- computerized authentication;
  - authentication credentials management;
  - use of an authorization 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, unauthorized access and specific software;
  - backup copies and restoring data and system availability;
  - keeping an up-to-date security policy document (exceptions to this duty are provided for by the Privacy Code); and
  - encryption or identification codes for specific processing operations performed by health-care bodies in respect of data disclosing health and sex life.
- 7.3 The Code also has specific security requirements where personal data is processed without electronic means (again contained in Annex B of the Code):
- regular updates 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 organizational departments;
  - procedures for the safekeeping of records and documents; and
  - procedures to keep certain records in restricted-access filing systems and access mechanisms to identify those entitled to have access.
- 7.4 Certain data controllers are allowed to implement simplified security measures.

## **8. Breach Notification**

There is no general obligation to notify data subjects or the Italian DPA about security breaches. There is one exception: the provider of a publicly available electronic communications service

(which would include telcos, mobile network operators and IISPs) must notify their users and the Italian DPA and the Italian telecommunications regulator of a risk of unauthorized access (*i.e.*, a security risk triggers the obligation, and not an actual data breach). An indication of the likely costs involved should also be communicated.

## 9. Enforcement & Penalties

9.1 The authority to investigate complaints, impose sanctions, appoint experts and all incidental powers lies with the DPA. However, the DPA must notify the public prosecutor in instances of criminal actions.

9.2 **Administrative and Criminal Sanctions.** The Code provides specific sanctions for administrative fines. The Code provides specific criminal sanctions carrying prison sentences. For instance:

- not registering with the DPA (where registration is required) – a fine of €20,000 – €120,000;
- failure to provide information requested by the DPA – a fine of €10,000 – €60,000;
- processing personal data without consent (where consent is required) €10,000 – €60,000;
- failing to provide or providing adequate information to data subjects may result in a fine of between €6,000 – €36,000. This may be increased by up to three times if found to be ineffective on account of the offender's economic status;
- failure to provide the minimum security measures – imprisonment of up to two years or a fine of €10,000 – €120,000;
- failure to comply with directions of the Italian DPA imprisonment of between six months and two years.

Fines can be increased by up to four times where they would otherwise be ineffective because of the data controller's size or in the case of serious breaches.

Where certain violations are less serious with regard to the social and/or business features of the activity at issue, the minimum to maximum fines set forth may be reduced by two-fifths.

When certain provisions are violated repeatedly and on different occasions, in connection with particularly large or important databases, a fine will be applied ranging from €50,000 to €300,000. Reduction of this fine will not be allowed.

In 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 minimum to maximum fines will be doubled.

9.3 The Italian DPA may carry out investigations and inspections to verify compliance with the Code either *ex officio*, or upon a third party's complaint.

Depending on the case, the DPA can "invite" the investigated entity to adopt compliance measures before issuing any sanction; this is usually more likely to

happen for minor breaches, and when investigations are commenced *ex officio*, whereas *ex parte* complaints are more likely to trigger actual sanctions.

The DPA does not have criminal prosecution powers, which are exclusive to the Judiciary, and resorting to criminal sanctions is extremely unusual, most cases leading to the imposition of fines. The most often targeted entities are telcos, e-commerce operators and IISPs, which have been subject to significant fines (in the range of several hundred thousand Euros).



## 1. Applicable Law

The Act on the Protection of Personal Information (the “Act”), was enacted in 2003 and became effective as to both public and private entities on April 1, 2005. The Act consists of a set of general guidelines, but not laws, governing the treatment of personal information in Japan, and delegates rulemaking authority to Japan’s government ministries, which in turn issue administrative guidelines for the business sectors for which each ministry is responsible.

<http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf> (Unofficial English Translation)

The activities of most businesses are covered by the guidelines promulgated by at least one of the following agencies:

- The Ministry of Economy, Trade, and Industry (“METI”).
- The Ministry of Health, Labour and Welfare (“MHLW”).<sup>8</sup>
- The Financial Services Agency (“FSA”).<sup>9</sup>
- The Ministry of Internal Affairs and Communications (“MIAC”).<sup>10</sup>
- The Ministry of Land, Infrastructure and Transport (“MLIT”).

While all ministry guidelines must abide by the Act, the guidelines promulgated by each ministry are not necessarily consistent with one another. In 2007, there were as many as 35 sets of guidelines issued pursuant to the Act, covering 22 business areas.

On May 24, 2013, the LDP-led ruling coalition directed the passage of the “Common Number” Bill (originally proposed in 2009) through both Diet chambers. The Common Number Bill plans to assign every Japanese resident, including mid-to-long-stay foreigners and special permanent residents, a personal identification number beginning in January 2016. Additionally, a portal site through which people can check their social security records and other information via the Internet is planned for 2017.

To oversee some aspects of the ID system, a third-party independent committee with independent authority will oversee allegations of data mishandling by public officials. Those who leak or illegally commercialize ID information will face up to four years in prison or a ¥2 million fine. While the use of a single number system has raised some concerns, including the potential for “forcible data-matching,” the government push for support has focused on efficiencies in administration and easier detection of tax evasion and welfare fraud.

On June 24, 2014, the Government of Japan, through its Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (“IT Strategic Headquarters”) presented its “Outline of the System Reform Concerning the Utilization of Personal Data” in the face of so-called “BigData” concerns. Commentators have noted that this proposed Revision to PIPA will remove most privacy protections from “reduced identifiability data” in a self-regulatory scheme with minimal enforcement considerations, no Japanese

<sup>8</sup><http://www.mhlw.go.jp/english/wp/wp-hw2/part2/p2c11s4.pdf>.

<sup>9</sup>[http://www.fsa.go.jp/frtc/kenkyu/event/20070424\\_02.pdf](http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf).

<sup>10</sup>[http://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/eng/Resources/others/110214\\_1.pdf](http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/others/110214_1.pdf).

Ministerial orders or prosecutions, and little transparency. This Revision to PIPA will be submitted during the ordinary session of the Diet in 2015.

## 2. Data Protection Authority and Registration Requirements

- 2.1 Japan has no central Data Protection Authority or registration requirements.
- 2.2 Each government ministry issues its own administrative guidelines in accordance with the general principles described in the Act and may adopt registration requirements that may or may not relate to the Act.
- 2.3 Many ministry guidelines call for voluntary participation from businesses in the business sectors governed by each entity.<sup>11</sup>

## 3. Protected Personal Data

- 3.1 **Personal information** is defined under the Act as information about a living individual, which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).
- 3.2 Personal Information Database is defined under the Act as
  - an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; or
  - an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved.
- 3.3 **Business Operator Handling Personal information** is defined under the Act as a business operator using a personal information database for its business; however, the following entities shall be excluded;
  - State organizations;
  - local governments;
  - incorporated administrative agencies, *etc.* (which means independent administrative agencies);
  - local independent administrative institutions (which means local incorporated administrative agencies); and
  - entities specified by a Cabinet Order as having little likelihood of harming the rights and interests of individuals considering the volume and the manner of utilization of personal information they handle.
- 3.4 **Personal data** is defined under the Act as personal information constituting a personal information database.

---

<sup>11</sup> The MHLW guidelines state that personal information protection can only be achieved by the voluntary participation of governed businesses. <http://www.mhlw.go.jp/english/wp/wp-hw2/part2/p2c11s4.pdf>.

- 3.5 **Retained Personal Data** is defined under the Act as such personal data over which a business operator handling personal information has the authority to disclose, to correct, add or delete the content, to discontinue its utilization, to erase, and to discontinue its provision to a third party, excluding the data which is specified by a Cabinet Order as harming public or other interests if its presence or absence is known and the data which will be erased within a period of no longer than one year that is specified by a Cabinet Order.
- 3.6 **Person** is defined under the Act as a specific individual identified by personal information.

#### 4. **Data Collection and Processing**

- 4.1 A business operator handling personal data shall not acquire personal information by deception or other wrongful means.
- 4.2 Specification of the Purpose of Utilization
- When handling personal data, a business operator handling personal information shall specify the purpose of utilization of personal information as much as possible.
  - The business operator handling personal data shall not change the purpose of utilization beyond the scope of the original purpose of utilization.
- 4.3 When a business operator handling personal data acquires personal data, it must notify the person of the purpose of utilization or publicly announce the purpose of utilization.
- 4.4 A business operator handling personal data shall not handle personal data about a person beyond the purpose of utilization without first receiving the consent of the person.
- 4.5 The [MHLW](#) has promulgated guidelines specifically addressing employee data. These guidelines mirror the Act's structure and consent requirements as applied to employees.

#### 5. **Data Sharing and Data Transfer**

- 5.1 An entity is forbidden from transferring personal data to third parties without the prior consent of the person, except in the following circumstances:
- the transfer is required by law;
  - the transfer is required to protect the person's life, bodily safety, or property, and obtaining the person's consent would present undue hardship;
  - the transfer is required to promote public health or positive child development, and obtaining prior consent of the person would present undue hardship; or

- the transfer is required for agents of national institutions and local public entities to perform their duties, and obtaining prior consent of the person presents undue hardship.
- 5.2 At the request of a data subject and except in limited circumstances, the business operator must cease providing personal data to third parties and notify the data subject of the application of any exception.
- 5.3 Prior to sharing or transferring personal data with a third party, the entity must provide the person with notice or place the person in circumstances where the person can easily learn of the following pieces of information and prevent the transfer:
- that the provision of the data to the third party is encompassed in the purpose of utilization;
  - the specific contents of the personal data to be provided;
  - the means or methods of providing the personal data to the third party; and
  - that the provision to the third party will cease at the request of the person.
- 5.4 An entity may share personal data with its affiliated companies if the entity provides notice to the person or places the person in circumstances whereby the person can easily learn the following information:
- the fact that the personal data will be jointly used;
  - the items of the personal data to be used;
  - the parties that will jointly use the personal data;
  - the purpose of the joint use; and
  - the name of an individual with responsibility over the joint use.

## **6. Data Security**

The Act generally requires governed entities, via the specific requirements of each ministry, to adopt appropriate measures to enforce the third-party sharing, notification of purpose of utilization, and proper purpose of acquisition provisions of the Act. In addition, the Act includes the following provisions related to the accuracy and security of personal data:

- 6.1 a business operator handling personal information shall endeavor to maintain personal data accurately and up to date within the scope necessary for the achievement of the purpose of utilization.
- 6.2 a business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data.
- 6.3 when a business operator handling personal information has an employee or trustee handling personal information, it must exercise appropriate supervision over the employee or trustee to ensure the security and control of the information.

## **7. Breach Notification**

While there is no general breach notification rule included in the Act, some Ministry Guidelines, such as the METI guidelines, impose a mandatory requirement on governed businesses that all persons affected by the leakage or data loss be notified to the extent reasonably possible and that a report regarding the breach be filed with METI. Other guidelines merely recommend notification, while others are silent on the issue.

## **8. Other Considerations**

- 8.1 The Act provides that, upon the request of a person, an entity must disclose and deliver to the person making the request the personal data held by the entity without delay. However, in the following circumstances, an entity is not required to disclose the requested information in the following circumstances:
- a risk of injury to the life or bodily safety of the person or a risk of impinging on the rights of the person or a third party would exist as a result of the disclosure;
  - the disclosure and delivery would result in a material interference with the entity's operations; or
  - the disclosure and delivery would violate other laws.
- 8.2 With respect to retained personal data, an organization must make available in writing retention information, contact information, and the purpose of retention.
- 8.3 An entity must provide a person with an opportunity to revise, correct, supplement, or delete personal data in the event the personal data is inaccurate. A person may also request a cessation of the use or the deletion of personal data that is used outside the scope of the purpose of utilization.

## **9. Enforcement & Penalties**

A business operator handling personal information shall appropriately and promptly process complaints about the handling of personal information and should establish a system for achieving this purpose.

Failure to comply with the Act or the Guidelines promulgated by ministries relating to the Act will result in administrative penalties. A minister may issue a recommendation for corrective measures to be undertaken by an entity in breach of the Act or Guidelines. If an entity does not cooperate with the recommendation without justifiable grounds, the minister may issue further orders regarding rectification. Failure to comply with an order leaves an entity liable for a fine of not more than 300,000 Japanese yen, and could face up to six months of imprisonment.

## 1. Applicable Law

The 2002 Act relating to the protection of individuals in relation to the processing of personal data (Loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel) (the "Act") implemented the EU Data Protection Directive 95/46/EC. The Act came into force on December 1, 2002. It has been amended by laws on July 31, 2006, December 22, 2006, and July 27, 2007.

[http://www.cnpd.public.lu/fr/legislation/droit-lux/doc\\_loi02082002\\_en.pdf](http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf) (Unofficial English Translation of Coordinated Text of Act and amendments)

The Act applies where personal data is processed by a data controller established in Luxembourg (and the processing occurs in the context of that establishment) or where the data controller is not established in Luxembourg, or in any other Member State of the European Union, but uses processing resources situated in Luxembourg (other than for the purposes of transit). A data controller can be both a natural or legal person.

Where processing is carried out by an individual exclusively for personal or domestic activities the Act does not apply. Processing for criminal investigations and judicial proceedings are also exempt and fall under separate legislation.

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** The National Commission for the Protection of Data ("*Commission nationale pour la protection des données*") ("National Commission" or "Commission") enforces this Act. The French language website of the Commission can be found here [www.cnpd.public.lu](http://www.cnpd.public.lu).
- 2.2 **Registration.** Certain processing activities require prior notification to, and others prior authorization from, the National Commission before initiating data processing.
  - Prior authorization from the National Commission is only required in relation to some acts, these are those that incur risks to data subject's rights such as processing of genetic data.
  - Prior notification must be given unless an exemption applies. The following circumstances are exempt from notification: presence of a data protection officer appointed by the data controller, and processing purely to keep a register that is used for public information purposes only and accessible to the public. An amendment in 2007 allowed for further exemptions from prior notifications, such as management of job applications and salaries.

## 3. Protected Personal Data

- 3.1 **Personal Data.** Personal data is any information of any type in any media (including sound and image) that relates to an identified or identifiable individual. An identifiable individual is deemed to be one that can be identifiable, directly or

indirectly, when data is crossed with other data that is in or comes to the data controller's possession.

- 3.2 **Sensitive Personal Data.** Sensitive Personal Data relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual preference, including the processing of genetic data.

#### 4. Data Collection and Processing Requirements

- 4.1 The data subject's consent is required for processing unless the data processor is:

- complying with a legal obligation to which the data controller is subject;
- performing a task carried out in the public interest or in the exercise of the official authority of the data controller or in a third party to whom the data is disclosed;
- performing a contract to which the data subject is a party, or in respect of measures taken at the request of the data subject before the contract is entered;
- pursuing the legitimate interests pursued by the data controller, or the interests of a third party or parties to whom the data is disclosed, except where these interests are disproportionate to the restrictions on the data subject's freedoms and fundamental rights; or
- protecting the data subject's vital interests.

- 4.2 If the data controller is also an employer, data processing for the purposes of supervision at the workplace can only occur under certain circumstances referred to in the Employment Code.

- 4.3 In regards to sensitive personal data, processing may only occur if:

- there is express consent of the data subject;
- necessary to comply with the data controller's employment law obligations and specific rights;
- necessary to protect the vital interest of the data subject where consent cannot be obtained due to incapacity (legal or physical);
- the data has clearly been made public by the data subject;
- carried out by certain non-profit organizations with the consent of the data subject and on condition that the processing relates solely to members of that body or to persons who have regular contact with it;
- necessary for acknowledging, exercising or defending a legal right;
- necessary in the public interest for historical, statistical or scientific reasons without prejudice to the specific requirements for specific categories of data by health services; or
- authorized by Luxembourg regulations (relates mostly to criminal proceedings and investigations).



- 4.4 In addition, there are separate provisions regarding the processing: (i) of specific categories of data by health services, (ii) of genetic data and (iii) for supervision purposes.
- 4.5 A written agreement is compulsory between data controllers and processors (those with whom data controllers contract that will be processing data on their behalf) and must provide that processors only act on the instructions of data controllers and they are subject to the obligations that they themselves are.
- 4.6 The controller must choose a processor that provides sufficient guarantees as regards the technical and organizational security measures pertaining to the processing to be carried out.

## **5. Data Transfer**

- 5.1 Without further requirements being necessary, data can be transferred within the European Economic Area (EEA).
- 5.2 Data cannot be transferred outside the EEA unless the recipient country is deemed to have adequate levels of protection. Countries with an adequate level of protection include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.
- 5.3 There are however, other situations in which data may be transferred outside of the EEA even though there is no adequate level of protection. They are:
  - if the data subject has given his consent;
  - if necessary to perform a contract to which the data subject and the data controller are parties, or to enter into this agreement at the data subject's request;
  - if necessary to perform or conclude a contract with a third party that is in the interest of the data subject;
  - if necessary or legally mandatory for reasons of substantial public interest or for establishing, exercising or defending legal rights;
  - if necessary to protect the vital interest of the individual; or
  - if the data comes from a public register.
- 5.4 Additionally, the data controller could use adopting standard contractual clauses such as the EU Model Clauses or multinational companies that use binding corporate rules to allow the transfer of data within the international company group. In such a case, the data controller will have to obtain prior authorization from the National Commission in order to be able to transfer personal data.

## **6. Data Security**

- 6.1 Data controllers must take all appropriate technical and organizational measures to ensure there is no unlawful or unauthorized interference, accidental or unlawful damage, accidental loss, falsification, unauthorized dissemination or access to the data. These measures include preventing physical and virtual



unauthorized access to the data and monitoring of transmissions and availability of the data.

- 6.2 The National Commission may request details of these measures, which must be given within 15 days of the request.

## **7. Breach Notification**

There is no legal requirement under the Act to give notice of breaches to the data subject or to the National Commission. However, it may be advisable, in certain circumstances, to approach the National Commission in case of a breach, in order to find a suitable solution. In addition, electronic communications service providers have breach notification requirements under the Luxembourg law implementing the EU telecom package.

## **8. Enforcement & Penalties**

The Act provides for both criminal and administrative sanctions.

- 8.1 Criminal sanctions for violations of the Act range from imprisonment for eight days to one year and/or fines from €251 to €125,000. Fines can only be decided by a criminal court.
- 8.2 The National Commission can, however, impose administrative sanctions such as:
- alerting data controllers who have violated the obligations imposed upon them;
  - blocking, deleting or destroying data that has been subject to a processing operation contrary to the provisions of the Act;
  - imposing a temporary or definitive ban on a processing operation that is contrary to the provisions of the Act; and
  - ordering publication of the prohibition decision in full or in extracts in newspapers or by any other method, at the cost of the person sanctioned.

## 1. Applicable Law

On November 15, 2013, the Personal Data Protection Act (PDPA) of 2010 was entered into force, introducing an omnibus privacy regime in Malaysia for the first time. This new regulation carries a host of requirements, including registration with the Personal Data Protection Department of Malaysia (PDPD) for a number of industries, including (among others) banking and financial institutions. The PDPA also includes the threat of severe consequences for non-compliance, including “fines for companies and/or fines and imprisonment for directors and officers of the company.”

<http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf>

## 2. Data Protection Authority and Registration Requirements

- 2.1 Under the PDPA, a Personal Data Protection Commissioner (the “Commissioner”) is appointed to carry out the functions and powers of the PDPA, including receiving complaints about violations and issuing decisions after complaint investigation.
- 2.2 Under the PDPA, the Minister may specify a class of data users who will be required to register.

## 3. Protected Personal Data

- 3.1 **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;
- recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- 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 the data user, including any sensitive personal data and expression of opinion about the data subject.

- 3.2 **Commercial transaction** means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency.
- 3.3 **Sensitive personal data** includes any of the following: information as to the physical or mental health or condition; political opinions, religious belief or other

beliefs of a similar nature; the commission or alleged commission of any offense; or any other personal data as the Minister may determine.

#### **4. Data Collection and Processing**

4.1 Under the PDPA, data users are generally required to obtain the consent of data subjects prior to the processing of their personal data.

4.2 Under the PDPA, data users may process the personal data of a data subject if the processing is necessary for:

- the performance of a contract to which the data subject is a party;
- the taking of steps at the request of the data subject toward entering into a contract;
- compliance with any legal obligation to which the data user is a subject, other than a contractual obligation;
- the protection of the vital interests of the data subject;
- the administration of justice; or
- the exercise of any functions conferred on any person by or under any law.

Personal data shall not be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data users;
- the processing of the personal data is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive in relation to that purpose.

4.3 Processing of sensitive personal data requires:

- (a) explicit consent;
- (b) that the processing is necessary:
  - (i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment
  - (ii) in order to protect the vital interests of the data subject or another person in a case where:
    - (A) consent cannot be given by or on behalf of the data subject; or
    - (B) the data user cannot reasonably be expected to obtain the consent of the data subject;

- (iii) 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;
  - (iv) for medical purposes and is undertaken by:
    - (A) a healthcare professional; or
    - (B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;
  - (v) for the purpose of, or in connection with, any legal proceedings;
  - (vi) for the purpose of obtaining legal advice;
  - (vii) for the purposes of establishing, exercising or defending legal rights;
  - (viii) for the administration of justice;
  - (ix) for the exercise of any functions conferred on any person by or under any written law; or
  - (x) for any other purposes as the Minister thinks fit; or
- (c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

## **5. Data Sharing**

- 5.1 Under the PDPA, the data subject must provide consent before any personal data can be disclosed and the data must be disclosed for the purpose for which it was collected.
- 5.2 Under the PDPA, the data user can disclose personal data without consent and for a purpose other than the one the data was collected for if:
- the disclosure is necessary to prevent crime or for the purpose of investigations or is required or authorized by law or by an order of court;
  - the data user acted in reasonable belief that he/she had the legal right to disclose the personal data to another party;
  - the data user acted in reasonable belief that he/she would have had the consent of the data subject if the data subject had known of the disclosure of the personal data and the circumstances surrounding it; or
  - the disclosure was justified as being in the public interest under the circumstances, as determined by the Minister.

## 6. Data Transfer

- 6.1 Under the PDPA, a data user cannot transfer personal data to a jurisdiction outside of Malaysia unless the jurisdiction has been specified by the Minister, upon the recommendation of the Commissioner and by notification published in the *Gazette*.
- 6.2 Under the PDPA, a data user may transfer personal data outside of Malaysia (notwithstanding the above requirement of Commissioner approval) if:
- the data subject gives consent;
  - the transfer is necessary for the performance of a contract between the data subject and the data user;
  - the transfer is necessary for the conclusion or performance of a contract between the data user and a third party, which is entered into at the request of the data subject or is in the interest of the data subject;
  - the transfer is for the purpose of any legal proceedings or for obtaining legal advice;
  - the data user has reasonable grounds for believing that under all circumstances of the case, the transfer is for the avoidance of adverse action against the data subject and it's not practicable to obtain written consent and if it was practicable to obtain written consent, the data subject would have given it;
  - the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data in that place will not be processed in any manner inconsistent with the PDPA; or
  - the transfer is necessary to protect the data subject's vital interest or is necessary as being in the public interest as determined by the Minister.

## 7. Data Security

Under the PDPA, a data user must take practical steps to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosures, or alteration or destruction.

## 8. Breach Notification

The PDPA does not require notification to any data subject or any other entity upon a breach.

## 9. Other Considerations

The PDPA provides individuals various rights regarding their personal data, including the following:

- right of access (a data user must respond to a request for access within 21 days);
- right to correct personal data;
- right to withdraw consent to the processing of personal data;
- right to prevent processing likely to cause damage or distress; and
- right to prevent processing for purposes of direct marketing.

## **10. Enforcement & Penalties**

- 10.1 Under the PDPA, the Commissioner can implement and enforce the provisions of the PDPA. In addition, violations of the PDPA can lead to criminal charges, potentially resulting in fines and/or imprisonment.
- 10.2 Directors, CEOs, COOs, managers, and other similar officers are jointly and severally liable for harm resulting from violation of the PDPA, subject to the usual due-diligence defense.
- 10.3 There is no express right for a data subject to pursue a civil claim against a data user for a breach of the PDPA.

## 1. Applicable Law

- 1.1 On July 6, 2010, Mexico enacted the Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de Particulares) (“Federal Law”). Regulations under the Federal law were issued on December 22, 2011.

[http://www.dof.gob.mx/nota\\_detalle.php?codigo=5150631&fecha=05/07/2010](http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010)

[http://dof.gob.mx/nota\\_detalle.php?codigo=5226005&fecha=21/12/2011](http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011)

- 1.2 On May 29, 2014, Mexico’s Economic Secretary promulgated “Parameters of Self-Regulation for the Protection of Personal Data,” which gave Mexico’s Federal Institute (discussed below) the authority to:

- Recognize codes of conduct for data protection; and
- Develop a process to recognize organizations which can become certifying bodies for those codes

[http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Parametros%20de%20Autor regulacion.pdf](http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Parametros%20de%20Autor%20regulacion.pdf)

[News reports](#) indicate that Mexico is debating new data protection and freedom of information laws, which are expected to be enacted in late 2014 or early 2015.

## 2. Data Protection Authority and Registration Requirements

- 2.1 Mexico’s data protection authority is the Federal Institute for Access to Public Information and Data Protection (Instituto Federal de Acceso a la Información Pública y Protección de Datos) (“Federal Institute”).

- 2.2 There are no registration requirements.

## 3. Protected Personal Data

- 3.1 **Personal information** refers to any information concerning an identified or identifiable individual.
- 3.2 **Sensitive personal information** includes personal information relating to the most private areas of the data owner’s life, or personal information which if misused might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive personal information is information that may reveal information such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, or sexual preferences.

## 4. Data Collection and Processing

4.1 In order to collect and process data, the data or personal information controller, which is the individual or private legal entity that decides on the processing of personal data, must provide a Privacy Notice (the “Notice”). The Notice should:

- be available to a data subject prior to collection and processing; and
- be provided in a certain manner, such as through print, digital, audio or visual format.

Further, the Privacy Notice must contain:

- the identity and domicile of the data controller collecting the data;
- the purposes of the data processing;
- the means the data owner has to exercise its right of access, rectification, cancellation, or opposition;
- the means for exercising rights of access, rectification, cancellation or objection, in accordance with other provisions of the Federal Law;
- where appropriate, the data transfers to be made; and
- the procedure and means by which the data controller will notify the data owner.

4.2 The processing of personal data must be limited to the fulfillment of the purposes set out in the Notice. If the data is used for another purpose, further consent of the data subject is required.

4.3 Consent is required for processing of data unless otherwise provided by law. Express written consent is required for processing sensitive personal data. Consent for processing of personal data will not be necessary where:

- any Law so provides;
- the data is contained in publicly available sources;
- the data has been anonymized;
- the data has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller;
- there is an emergency situation that could potentially harm an individual’s well-being or property;
- it is essential for medical attention, prevention, diagnosis, health-care delivery, medical treatment or health-services management and the data subject is unable to give consent; or
- a resolution waiving the consent requirements is issued by a competent government authority.

Implicit consent applies to the processing of personal data provided notice has been provided and there has been no objection.

Express consent is required for the processing of financial or asset data and the processing of sensitive personal data.



- 4.4 The data subject may cancel his or her personal data at any time, but a data controller is not obligated to cancel personal data when:
- it relates to parties to a private or administrative contract or partnership agreement and is necessary for performance and enforcement of the contract;
  - the law requires that it be processed;
  - cancellation would hinder judicial or administrative proceedings relating to tax obligations, investigation and prosecution of crimes, or updating of administrative sanctions;
  - it is necessary to protect the legally protected interests of the data owner;
  - it is necessary to carry out an action in the public interest;
  - it is necessary to fulfill an obligation legally undertaken by the data owner; or
  - it is subject to processing for medical diagnosis or prevention or health services management.

## 5. Data Transfer

- 5.1 Data can be processed by a third party so long as he or she is in compliance with all the requirements the data controller must comply with in collecting and processing data under the Federal Law.
- 5.2 All transfers of personal data to domestic or foreign third parties require the disclosure of the Notice and require the data subject's consent. Consent is not required in the following circumstances:
- where the transfer is pursuant to a law or treaty to which Mexico is party;
  - where the transfer is necessary for medical diagnosis or prevention, health-care delivery, medical treatment or health-services management;
  - where the transfer is made to holding companies, subsidiaries or affiliates under common control of the 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;
  - where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;
  - where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
  - where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding; or
  - where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner.
- 5.3 The recipient of personal data is subject to the same conditions as the data controller and must be provided with the Notice.

## **6. Data Security**

- 6.1 The data controller and all parties that process personal data must establish and maintain physical, technical, and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing.
- 6.2 Data controllers must adopt security measures equal or superior to those they use to manage their own information.
- 6.3 The sufficiency of the data controller's security measures will be assessed relative to the following factors:
- the inherent risk posed by the type of personal data;
  - the potential consequences of a breach for the data subject;
  - the sensitivity of the data;
  - the number of data subjects;
  - pre-existing vulnerabilities in the processing system;
  - the value the data may have for an unauthorized third party;
  - technological developments; and
  - other facts impacting the risk level.
- 6.4 The data controller or third parties involved in any stage of personal data processing must maintain confidentiality with respect to such data, and this obligation will continue even after the end of his or her relationship with the data owner or data controller.
- 6.5 The Federal Institute may also issue recommendations to data controllers for securing data when the data controller's security measures are insufficient or may put the personal data at risk.

## **7. Breach Notification**

- 7.1 Security breaches that "materially" affect property or personal rights must be reported immediately to the affected individuals so that they may take actions to defend their rights. The notification must provide at least the following information:
- the nature of the violation;
  - the personal data comprised;
  - the corrective actions implemented; and
  - the means by which the data subject may obtain more information regarding the breach.
- 7.2 The data controller must immediately analyze causes of the breach and implement corrective, preventive, and improvement security actions.

## **8. Other Considerations**

- 8.1 All information processed in Mexico is subject to the Federal Law regardless of the location of its customers, but information simply passing through Mexico is not subject to the Federal Law.

## **9. Enforcement & Penalties**

- 9.1 The Federal Institute may act on its own or in response to complaints regarding violations of the Federal Law or Regulations.

- 9.2 Violations of the Federal Law may result in monetary penalties according to the following terms:

- a warning instructing the data controller to carry out the actions requested by the data owner, under the terms established by this Law;
- a fine of between 100 to 160,000 days of Mexico City's minimum wage;
- a fine of between 200 to 320,000 days of Mexico City's minimum wage; or
- in the event of repeated occurrences of violations, an additional fine of between 100 to 320,000 days of the Mexico City's current minimum wage will be imposed. With regard to violations committed in processing sensitive data, sanctions may be increased up to double the established amounts.

- 9.3 Imprisonment may occur for the unlawful processing of personal data according to the following terms:

- three months to three years imprisonment will be imposed on any person who, authorized to process personal data for profit, causes a security breach affecting the databases under his/her custody;
- six months to five years imprisonment will be imposed on any person who, with the aim of achieving unlawful profit, processes personal information; or
- for the unauthorized processing of sensitive personal information, imprisonment ranging from three to six years and a fine of between two million and five million pesos.

- 9.4 Data owners who feel they have suffered harm or damage to their rights or property as a result of a breach of the provisions of the Act may exercise the rights they deem appropriate for purposes of any applicable indemnity in the terms of the relevant law.

## 1. Applicable Law

The Act on the Protection of Personal Data 2000 implements EU Data Protection Directive 95/46/EC (the “Act”). The Act came into effect on September 1, 2001.

<http://www.legislationline.org/documents/id/5342> (Unofficial English Translation)

[http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum\\_17-03-2013](http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_17-03-2013)

On February 19, 2013, the DPA published new guidelines on the protection of personal data. These guidelines discuss in further detail the security measures required under the Act.

A summary of the guidelines is provided in English here:

[http://op.bna.com/pl.nsf/id/dapn-95akt4/\\$File/englishtulips.pdf](http://op.bna.com/pl.nsf/id/dapn-95akt4/$File/englishtulips.pdf)

The Act applies to all processing of personal data conducted within the scope of the operations of an establishment of the data controller in the Netherlands, regardless of where the data are processed or where the data subjects are. If the data controller is established in another EU Member State, that Member State’s legislation applies.

The Act also applies to all processing of personal data when the data controller is not established in the EU, but uses equipment situated in the Netherlands to process personal data (other than for the purposes of transit). Data processing in that case is only allowed when the data controller has appointed a representative in the Netherlands that acts and complies with the provisions of the Act on his behalf.

## 2. Data Protection Authority and Registration Requirements

- 2.1 **Authority.** The Act is supervised by the Dutch Data Protection Authority, whose English language website is here: <https://cbpweb.nl/en>.
- 2.2 **Registration.** The Dutch DPA must be notified of all processing of personal data in whole or in part by automatic means.
- 2.3 The notification must contain:
  - name and address of the responsible party;
  - purpose or purposes of the processing;
  - description of the categories of data subjects and of the data or categories of data relating thereto;
  - recipients or categories of recipients to whom the data may be supplied;
  - planned transfers of data to countries outside the European Union; and
  - general description of security measures in place.
- 2.4 An exemption from DPA notification applies in certain cases. If the data controller complies with further restrictions as set forth in the Exemption Decree to the Act, a DPA notification is not required. Examples of exempt activities include data

processed on debtors and creditors, customers and suppliers, legal and accounting services, HR management, scientific research and statistics and document management.

### 3. Protected Personal Data

- 3.1 **Personal Data.** Personal data means any information relating to an identified or identifiable natural person.
- 3.2 **Sensitive Personal Data.** Sensitive Personal Data includes personal data concerning religion or philosophy of life, race, political persuasion, health and sexual life, or trade union membership, or criminal behavior, or unlawful conduct connected with a ban imposed with regard to such conduct.

### 4. Data Collection and Processing

4.1 Personal data may be processed where:

- data subject has unambiguously given consent;
- necessary for the performance of a contract to which the data subject is a party, or pre-contractual measures to be performed at the request of data subject;
- necessary in order to comply with a legal obligation to which the responsible party is subject;
- necessary in order to protect a vital interest of the data subject;
- necessary for the proper performance of a public law obligation by the administrative body concerned or by the administrative body to which the data are given; or
- necessary for pursuing legitimate interests of the responsible party or of a third party to whom the data are supplied, except where the rights and freedoms of the data subject prevail.

4.2 Processing of sensitive personal data is prohibited unless certain circumstances apply:

- express consent of the data subject;
- data have been manifestly made public by the data subject;
- necessary for the establishment, exercise or defense of a legal right; necessary to protect the vital interests of the data subject or a third party and it is impossible to obtain permission;
- it is necessary to comply with an obligation of international public law;
- it is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy and this is provided by law or else the DPA has granted an exception (to which the DPA can impose rules and restrictions). In this instance, the processing must give notice to the European Commission; process by the College or an ombudsman referred to in Article 9:17 of the General Administrative Law Act for certain enumerated purposes
- the general prohibition for processing sensitive personal data does not apply where carried out for the purpose of research or statistical use if:

- research serves a public interest;
- processing is necessary for the research or statistics concerned;
- it appears to be impossible or would involve a disproportionate cost to ask for express consent; and
- sufficient guarantees are given that the processing does not adversely affect the rights and freedoms of the individual to a disproportionate extent; or
- amendments to the Act (effective February 9, 2012) allow the processing of sensitive personal data where necessary to protect the vital interest of the data subject.

4.3 There are further restrictions on specific categories of data. For example:

- Data relating to religion or philosophy of life can be processed where carried out by church associations or associations founded on spiritual or philosophical principles.
- Data regarding the health of a data subject may be processed by medical and healthcare professionals where necessary for the treatment and care of the data subject. This is also extended to certain insurance companies as provided for by other areas of Dutch law where assessing risk to be insured by that insurance company, in regards to performing that insurance agreement. Schools may also process data regarding health of a data subject when providing special support.

## 5. Data Processing

- 5.1 A written contract between the data controller and the processor is mandatory.
- 5.2 The data controller has to make sure that the processor provides adequate guarantees with respect to technical and organizational security measures for the processing to be carried out. The data controller makes sure that these measures are complied with.
- 5.3 The data controller must ensure that the processor (a) processes the personal data in accordance with the provision that itself and anyone acting under the authority of the data controller or the processor only process such data on the orders of the data controller, except as required by law; and (b) complies with the same security obligations incumbent upon the data controller.
- 5.4 If the processor is established in any other EU member state, the data controller has to make sure that the processor complies with that member state's data protection laws.

## 6. Data Transfer

- 6.1 Without further requirements, international transfers are permitted within the European Economic Area (EEA).
- 6.2 Transfers are permitted outside of the EEA where the recipient country has adequate levels of protection. Countries with an adequate level of protection

include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. Transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

- 6.3 Where there are no adequate guarantees, data may be transferred outside the EEA where:
- the data subject has given their unambiguous consent;
  - it is necessary for the performance of a contract between the data subjects and the responsible parties, or for pre-contractual measures to be carried out;
  - it is necessary for the conclusion or performance of a contract concluded or to be concluded between responsible parties and third parties in the interests of data subjects;
  - it is necessary on account of an important public interest, or for the establishment, exercise or defense in law of any right;
  - it is necessary to protect a vital interest of data subjects; or
  - it is carried out from a public register set up by law or from a register which is accessible by the public.
- 6.4 A permit may be issued by the Minister of Justice, after having consulted the Dutch DPA, for a personal data transfer or category of transfers to a non-member country that does not provide guarantees of an adequate level of protection. Attached to such permit are the more detailed rules required to protect among others individual privacy. The request for a permit needs to be filed through the Dutch DPA. Processing data before a permit has been issued, is not permitted. The permit does not alter other obligations resulting from the Act.
- 6.5 The DPA was amended effective February 9, 2012, which dispensed with the requirement to obtain a permit issued by the Minister of Justice where standard contractual clauses approved by the European Commission are used. The amendment is meant to deal with the delays in obtaining such a permit.
- 6.6 The above, however, does not imply that only the use of model clauses is allowed. Other means, like contractual clauses not based on the model clauses that provide an adequate level of protection, are permitted. The Dutch DPA verifies whether the contractual clauses provide at least the same level of protection as the model clauses, before advising the Minister of Justice, and a permit will likely be required.
- 6.7 Binding corporate rules (“BCRs”) can be used under Dutch law to provide guarantees for an adequate level of protection. BCRs need to be reviewed by the Dutch DPA. In reviewing BCRs, the Dutch DPA follows the guidelines as set out by the European Article 29 Data Protection Working Party. The implementation of BCRs is not a substitute for compliance with the Act, and should not be considered as an instrument to replace (parts of) the Act.



## 7. Data Security

The data controller must ensure appropriate technical and organizational measures are used to ensure that personal data is protected against loss from any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data. (Article 13)

The DPA Guidelines clarify that the Article requires organizations to follow the “Plan-Do-Check-Act” cycle. This involves assessing the risks, using generally accepted security standards, and checking and evaluating the security measures regularly.

## 8. Breach Notification

There is currently no notification requirement for breach under the Act. However, amendments to the European data protection legislation may result in the addition of a notification requirement to the Act. As of June 1, 2012, the Dutch Telecommunications Act incorporated a breach notification requirement applicable to Internet service providers and providers of public telecommunications networks. Every security breach that might pose a risk to the protection of personal data has to be notified to the Dutch DPA.

## 9. Enforcement & Penalties

- 9.1 Parties who deliberately commit an offense can face a prison sentence for a maximum of 6 months or a fine. Criminal prosecution can only be started by the Public Prosecutor, not on the sole initiative of the Dutch DPA. The February 2012 Amendment increased the potential fines – up to a maximum of €19,000 – for failing to register the processing of personal data with the governing authority, or for intentional acts of omission.<sup>12</sup>
- 9.2 The Dutch DPA has the authority to impose periodic penalty payments to enforce the Act. A failure to notify the Dutch DPA may result in an administrative fine of up to €4,500.
- 9.3 In addition to the Act, the Dutch DPA also supervises compliance with the Police Data Act and the Municipal Database (personal files) Act. The Dutch DPA serves mainly as an advisory body for data controllers and data protection officers. It promotes self-regulation and encourages companies to formulate a code of conduct for their branch of industry or sector.
- 9.4 As the Dutch DPA strongly relies on self-regulation, this is also reflected in their practical approach to enforcement. Based on publicly available documents and letters, the Dutch DPA usually approaches businesses to encourage compliance before they resort to penalties. This is currently usually done by official inquiries and recommendations, followed by a summons to cease the infringement(s), on pain of a penalty. This practice may change in the future.

---

<sup>12</sup> [http://www.loc.gov/lawweb/servlet/lloc\\_news?disp3\\_l205403124\\_text](http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403124_text)



## 1. Applicable Law

Peru adopted Law N° 29733, the Personal Data Protection Law (the “Law”) in July 2011. The Law is available here in Spanish:

<http://www.jovenesalaobra.gob.pe/Descargas/transparencia/LEY-29733.pdf>

An English translation of the Law is available here:

[http://web.ita.doc.gov/ITI/itiHome.nsf/1dd3c7c4faeeff0585256ccb00657bab/112a1a2f4d01989c85257a78004dd2ec/\\$FILE/Peru%20Data%20Protection%20Law%20July%2028\\_EN.pdf](http://web.ita.doc.gov/ITI/itiHome.nsf/1dd3c7c4faeeff0585256ccb00657bab/112a1a2f4d01989c85257a78004dd2ec/$FILE/Peru%20Data%20Protection%20Law%20July%2028_EN.pdf).

On March 22, 2013, the Law came into effect - 30 days after the Peruvian government published implementing regulations. The implementing regulations are available in Spanish here:

<http://spij.minjus.gob.pe/normas/textos/220313T.pdf>

## 2. Data Protection Authority and Registration Requirements

- 2.1 National Authority for Personal Data Protection (through the National Department of Justice) (the “Authority”).

National Register of Personal Data Protection—A data controller who processes personal data must notify the National Authority for Personal Data Protection, which keeps a public register of data processors and the type of data they collect.

## 3. Protected Personal Data

- 3.1 **Personal data** is defined by the Law as any information on an individual which identifies or makes him/her identifiable through means that may be reasonably used.
- 3.2 **Sensitive personal data** means any of the following: biometric data, data concerning the racial and ethnic origin; political, religion, philosophical or moral opinions or convictions, personal habits, union membership and information related to health or sexual life.

## 4. Data Collection and Processing

- 4.1 Unless otherwise exempted by statute, data controllers are generally required to obtain the consent of data subjects for the processing of their personal data. Consent must be prior, informed, express and unequivocal.
- 4.2 In the case of sensitive personal data, consent must also be given in writing, which may be done digitally. Even without the consent of the subject, sensitive data may be processed when authorized by law, provided that it is in the public interest.

4.3 Data controllers may process personal data without consent:

- when the personal data are compiled or transferred for public entities in control of the personal data and in the performance of its duties;
- when personal data is accessible to the public or is intended to be accessible to the public;
- to comply with other laws related to financial solvency and credit;
- in the case of a law for the promotion of competition in regulated markets under certain circumstances;
- when necessary to perform a contract to which the data subject is a party;
- for personal data related to health, under certain circumstances;
- when processing is carried out by non-profit organizations with political, religious or union purposes, under certain circumstances; or
- in an anonymization or disassociation procedure.

**5. Data Transfer**

5.1 A data controller may transfer personal data to places outside of Peru only if the recipients have adequate protection measures. The National Authority for the Protection of Personal Data will supervise compliance with this requirement.

5.2 That provision does not apply in the following cases:

- when the data subject has given his/her prior, informed, express and unequivocal consent;
- agreements under international treaties to which Peru is a party;
- international judicial cooperation;
- international cooperation between intelligence agencies for the fight against terrorism, illegal drug trafficking, money laundering, corruption, human trafficking and other forms of organized crime;
- when necessary to implement a contract to which the data subject is a party;
- to comply with laws concerning the transfer of bank or stock exchanges; or
- when the transfer is for the prevention, diagnosis or medical or surgical treatment of the data subject; or when necessary to carry out epidemiological or similar studies (provided that adequate disassociation procedures are applied).

**6. Data Security**

6.1 Data controllers must adopt technical, organization and legal measures to guarantee the security of personal data and avoid their alteration, loss, unauthorized processing or access.

**7. Breach Notification**

7.1 Peru's law does not require any notifications to any data subject or any other entity upon a breach.

## 8. Other Considerations

8.1 Peru's law mandates special regulations be enacted for the processing of personal data of minors.

8.2 Peru's law provides individuals various rights to their personal data:

- right of access;
- right to information;
- right of update, inclusion, rectification and elimination;
- right of opposition;
- right to prevent the data from being supplied;
- right not to be subject to a decision with legal effects on him/her or affecting him/her significantly, supported only by a processing of personal data intended to evaluate certain aspects of his personality, unless it occurs under certain conditions;
- right to protection: allows a data subject to appeal directly to the Authority in case of a violation of their rights; and
- right to be indemnified: provides for unspecified compensation by the entity responsible for violation of the law.

## 9. Enforcement & Penalties

9.1 The Authority is the primary enforcer of the law and can issue the following administrative sanctions (fines) based upon whether the violation is mild, serious or very serious:

- mild violations will be sanctioned with a minimum fine of 0.5 Tax Units up to -five Tax Units;
- serious violations will be sanctioned with a fine of more than five Tax Units up to 50 Tax Units;
- very serious violations will be sanctioned with a fine of more than 50 Tax Units up to 100 Tax Units;
- the fine imposed may not exceed under any circumstances 10% of the annual gross income received by the presumed violator during the previous fiscal year.

9.2 The law provides a "Principle for availability of recourse for the data subject" stating that any data subject must have the administrative and/or jurisdictional channel necessary to claim and enforce his rights when they are violated by the processing of his personal data.

## 1. Applicable Law

On March 20, 2012, the Senate of the Philippines passed the Data Privacy Act of 2012 (the “Act”), also known as “An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Data Protection Commission, and for Other Purposes.” The Act became effective on October 1, 2012. The official text of the Act can be found here:

<http://www.gov.ph/2012/08/15/republic-act-no-10173/>

In related legislation, the [Philippines’ Supreme Court signed](#) the [Cybercrime Prevention Act](#) into law on February 18, 2014. This law contributes additional protections to data within the Philippines by [adding protections against illegal access and interception of data](#), and also incorporates online libel punishments.

## 2. Data Protection Authority and Registration Requirements

- 2.1 The Philippines’ data protection authority is the National Privacy Commission (the “Commission”).
- 2.2 There are no registration requirements, except for government agencies entering into any contract with a government contractor that may involve accessing or requiring sensitive personal information from 1,000 or more individuals. In this case, the agency shall require a government contractor and its employees to register their personal information processing system with the Commission in accordance with the Act.

## 3. Protected Personal Data

- 3.1 **Personal information** refers to any information, regardless of whether it is recorded in a material form, 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.
- 3.2 **Sensitive personal information** includes personal information: (1) about an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2) about an individual’s health, education, genetic or sexual life, or any proceeding for any offense committed or alleged to have been committed by such person, the disposition of such proceedings, or the sentence from any court in such proceedings; (3) issued by government agencies uniquely to an individual which includes, but is not limited to, Social Security numbers, previous or current health records, licenses or its denial, suspension or revocation, and tax returns; and (4) specifically established by an executive order or an act of Congress to be kept classified.

## 4. Data Collection and Processing

4.1 Data may be collected and processed by a personal information controller (a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf) so long as the personal information is:

- 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, in certain circumstances, kept up to date;
  - Inaccurate or incomplete data must be rectified, supplemented, destroyed or its further processing restricted.
- adequate and not excessive in relation to the purposes for which it is 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 defense 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, unless the information is collected for certain uses.

In addition, at least one of the following conditions must exist:

- 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 a national emergency, to comply with the requirements of public order and safety, or to fulfill functions of a 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 in certain circumstances.

4.2 Sensitive personal information may not be collected and processed, except in very limited circumstances.

## **5. Data Transfer**

- 5.1 The personal information controller must ensure that third parties processing personal information on its behalf shall implement the security measures provided by the Act.
- 5.2 The personal information controller is responsible for information that has been transferred to a third party, whether domestically or internationally, subject to cross-border arrangement and cooperation.
- 5.3 The personal information controller is accountable for complying with the requirements of the Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party.

## **6. Data Security**

- 6.1 The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
- 6.2 The Act does not specify the exact protocols to be used, however 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 processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines that the Commission may issue from time to time, the measures implemented by the personal information controller must include at a minimum:
  - safeguards to protect its computer network against accidental, unlawful or unauthorized 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.

## **7. Breach Notification**

- 7.1 The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. 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 notification should at least describe the:

- nature of the breach;
- sensitive personal information possibly involved; and
- measures taken by the entity to address the breach.

7.2 In determining whether notification is warranted, the Commission may take into account compliance by the personal information controller with the notification requirements of the Act and the existence of good faith in the acquisition of personal information. Further, the Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects and may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

## **8. Other Considerations**

- 8.1 The Act provides data subjects a right of access to their personal information, a right to correct the information, and the right to lodge a complaint before the Commission.
- 8.2 The Act applies to personal information controllers who are not established in the Philippines, but who use equipment located in the Philippines, or maintain an office, branch or agency in the Philippines, provided certain conditions are met.
- 8.3 Although the Act does not contain cross-border data transfer restrictions, the Act applies to certain foreign processing of personal information about Philippines residents. However, the law will not apply to 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.

## **9. Enforcement & Penalties**

- 9.1 Unauthorized processing of personal information is punishable by imprisonment ranging from one to three years and a fine of between 500,000 and 2 million pesos.
- 9.2 Unauthorized processing of sensitive personal information is punishable by imprisonment ranging from three to six years and a fine of between 500,000 and four million pesos.
- 9.3 Improper disposal of personal information is punishable by imprisonment ranging from six months to two years and a fine of between 100,000 pesos and 500,000 pesos.
- 9.4 Improper disposal of sensitive personal information is punishable by imprisonment ranging from one to three years and a fine of between 100,000 pesos and 1 million pesos.



- 9.5 Negligently accessing personal information is punishable by imprisonment ranging from one to three years and a fine of between 500,000 pesos and 2 million pesos.
- 9.6 Negligently accessing sensitive personal information is punishable by imprisonment ranging from three to six years and a fine of between 500,000 pesos and 4 million pesos.
- 9.7 Processing personal information for an unauthorized purpose is punishable by imprisonment ranging from one year and six months to five years and a fine of between 500,000 pesos and 1 million pesos.
- 9.8 Processing sensitive personal information for an unauthorized purpose is punishable by imprisonment ranging from two to seven years and a fine of between 500,000 pesos and 2 million pesos.
- 9.9 Unauthorized access or an intentional breach is punishable by imprisonment of one year to three years and a fine of between 500,000 and 2 million pesos.
- 9.10 Concealment of a security breach involving sensitive personal information is punishable by imprisonment ranging from one year and six months to five years and a fine of between 500,000 and 1 million pesos.
- 9.11 Malicious disclosure of unwarranted or false information relative to any personal information or sensitive personal information is punishable by imprisonment ranging from one year and six months to five years and a fine of between 500,000 and 1 million pesos.
- 9.12 Unauthorized disclosure to a third party of personal information that is not covered by the immediately preceding section, without the consent of the data subject, is punishable by imprisonment ranging from one to three years and a fine of between 500,000 and 1 million pesos. Unauthorized disclosure to a third party of sensitive personal information that is not covered by the immediately preceding section, without the consent of the data subject, is punishable by imprisonment ranging from three to five years and a fine of between 500,000 and 2 million pesos.
- 9.13 Any combination or series of acts as defined by the Act is punishable by imprisonment ranging from three to six years and a fine between 1 million and 5 million pesos.
- 9.14 Extent of Liability
- If the offender is a corporation, partnership, or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or, by their gross negligence allowed, the commission of the crime.
  - The maximum penalty on the scale of penalties shall be imposed when the personal information of at least one hundred persons is harmed, affected or involved.



## 1. Applicable Law

The Qatar Financial Centre (“QFC”), a business and financial center created by the Qatar government, has promulgated a set of comprehensive data privacy protection regulations applicable to the entire country. The Qatar Data Protection Regulation (“DPR”), Law No. 7 of 2005, was implemented by Regulation No. 6 of 2005. The official text of the DPR is available here:

[http://www.complinet.com/net\\_file\\_store/new\\_rulebooks/q/f/QFCRA\\_1559\\_VER1.pdf](http://www.complinet.com/net_file_store/new_rulebooks/q/f/QFCRA_1559_VER1.pdf)

### Data Protection Authority and Registration Requirements

- 1.1 The DPR is administered by the Qatar Financial Centre Authority (“QFCA”).
- 1.2 Data Controllers are required to establish and maintain a record of their operations with respect to Personal Data, and the QFCA may promulgate rules requiring these entities to provide this record upon request.

## 2. Protected Personal Data

- 2.1 **Personal Data** is defined under the DPR as any information relating to an identified natural person or an Identifiable Natural Person.
- 2.2 **Identifiable Natural Person** is defined under the DPR as a natural 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 physical, physiological, mental, economic, cultural or social identity.
- 2.3 **Sensitive Personal Data** is defined under the DPR as Personal Data revealing or relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life.
- 2.4 **Data Subject** is defined under the DPR as the individual to whom Personal Data relates.

## 3. Data Collection and Processing

- 3.1 **Data Controller** is defined under the DPR as any person in the QFC who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
- 3.2 **Processing** is defined under the DPR as 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.

- 3.3 **Recipient** is defined under the DPR as a Person to whom Personal Data is disclosed, whether a third party or not; however, authorities which may receive Personal Data in the framework of a particular inquiry shall not be regarded as recipients.
- 3.4 Data Controllers must ensure that the Personal Data they Process is:
- processed fairly, lawfully and securely;
  - processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further processed in a way incompatible with the those purposes or rights;
  - adequate, relevant and not excessive in relation to the purposes for which it is collected or further Processed;
  - accurate and, where necessary, kept up to date; and
  - kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes it was collected or for which they are further processed.
- 3.5 A Data Controller must establish and maintain systems and controls that enable it to comply with the requirements of the DPR.
- 3.6 Personal Data may only be Processed if:
- the Data Subject has unambiguously given his 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 the Data Controller's compliance with any legal obligation;
  - 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 interests of the QFD or in the exercise of enumerated functions or power; 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 in certain circumstances.
- 3.7 Data Controllers must provide a Data Subject whose Personal Data it collects with at least the following information immediately upon commencing to collect Personal Data:
- the identity of the Data Controller;
  - the purposes of the Processing for which the Personal Data are intended; and
  - any further information needed to guarantee fair Processing in respect of the Data Subject, such as:
    - the Recipients or categories of Recipients of the Personal Data, unless the Data Controller reasonably expects that the Data Subject is already aware of that information;

- whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the Data Subject's right of access to and the right to rectify the Personal Data;
- whether the Personal Data will be used for direct marketing purposes; and
- whether the Personal Data will be Processed for other purposes.

3.8 Sensitive Personal Data cannot be Processed unless:

- the Data Subject has given his explicit consent to the Processing of that Personal Data;
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller in the field of employment law;
- 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 by a foundation, association, or any other non-profit-seeking body in certain circumstances;
- Processing is necessary for compliance with any legal obligation to which the Data Controller is subject;
- Processing is necessary to uphold the legitimate interests of the Data Controller recognized in the international financial markets, subject to certain conditions;
- Processing is necessary to comply with auditing, accounting or anti money-laundering obligations that apply to a Data Controller; or
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services provided certain conditions are met.

This article shall not apply if:

- a permit has been obtained to process Sensitive Personal Data from the QFC Authority; and
- The Data Controller applies adequate safeguards with respect to the processing of the Personal Data.

## 4. Data Transfer

### 4.1 Transfers out of the QFC

- A Data Controller may only transfer Personal Data to a Recipient located in a jurisdiction outside the QFC if an adequate level of protection for that Personal Data is ensured by laws and regulations that are applicable to the Recipient.
- The adequacy of the level of protection will be assessed in the light of all the circumstances surrounding the transfer, including but not limited to:
  - the nature of the data;
  - the purpose and duration of the proposed Processing operation or operations;

- if the data does not emanate from the QFC, the country of origin and country of final destination of the personal data; and
- any relevant laws to which the recipient is subject, including professional rules and security measures.
- Exception
  - A Data Controller may transfer Personal Data to a Recipient not subject to an adequate level of protection if:
    - the QFCA has granted a permit for the transfer and the Data Controller applies adequate safeguards;
    - the Data Subject has given his unambiguous consent to the proposed transfer;
    - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a third party
    - the transfer is necessary or legally required on grounds important in the interests of the QFC, or for the establishment, exercise or defense 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 laws or regulations is intended to provide information to the public and which satisfies other conditions;
    - the transfer is necessary for compliance with any legal obligation to which the Data Controller is subject;
    - the transfer is necessary to uphold the legitimate interests of the Data Controller recognized in the international financial markets, provided certain conditions are met; or
    - the transfer is necessary to comply with auditing, accounting or anti money laundering obligations that apply to a Data Controller which is established in the QFC.

## **5. Data Security**

- 5.1 The Data Controller must implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing.
- 5.2 Taking into account the cost of implementation, the security measures must ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected.
- 5.3 The Data Controller must, where Processing is carried out on its behalf, choose a Data Processor which provides sufficient guarantees of the technical security measures and organizational measures governing the Processing and ensure compliance with those measures.

## **6. Breach Notification**

- 6.1 The DPR does not impose a duty on Data Controllers to notify Data Subjects or the QFCA of a breach of their Personal Data.

## **7. Other Considerations**

### **7.1 Access, Rectification, Erasure, or Blockage**

- A Data Subject has the right to obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or response:
  - confirmation as to whether Personal Data relating to him/her is being processed and, if so, information regarding the Processing, categories of Personal Data concerned, and the Recipients to whom the Personal Data is disclosed;
  - a description in an intelligible form of the Personal Data undergoing Processing and its source; and
  - as appropriate, the rectification, erasure or blocking of Personal Data when the Processing does not comply with the DPR.

### **7.2 Objections**

- A Data Subject has the right to:
  - object at any time on reasonable grounds relating to his/her particular situation to the Processing of Personal Data relating to him/her; and
  - be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses.
- Where there is a justified objection, the Processing instigated by the Data Controller shall no longer include that Personal Data.

## **8. Enforcement & Penalties**

### **8.1 Directions**

- If the QFC Authority determines that a Data Controller has contravened or is contravening the DPR, it may issue an order requiring the Data Controller to do either or both of the following:
  - refrain from doing any act or thing within such time as may be specified in the direction; or
  - refrain from further 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.

### **8.2 Claims**

- A person who believes they have been adversely affected by a violation of the DPR may file a claim with the QFCA.
- On the basis of a complaint, the QFCA may issue a direction requiring the Data Controller to do any act or thing, and the Data Controller must comply with the direction.

## 1. Applicable Law

The Kingdom of Saudi Arabia (“KSA”) currently does not have a comprehensive data breach notification law in effect. There are, however, several sources of KSA law relevant to data, data privacy, and the obligations of those in possession of data.

Article 40 of the Saudi Arabian Constitution guarantees citizens privacy in their communications unless otherwise provided for by statute or royal decree.

[http://www.saudiembassy.net/about/country-information/laws/The\\_Basic\\_Law\\_Of\\_Governance.aspx](http://www.saudiembassy.net/about/country-information/laws/The_Basic_Law_Of_Governance.aspx)

The Telecommunications Act of 2001 and the Anti-Cyber Crime Law of 2007 provide penalties for wrongfully accessing or disclosing data. The original text of the Telecommunications Act is provided in Arabic here: [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=207021](http://www.wipo.int/wipolex/en/text.jsp?file_id=207021)

An Unofficial English Translation is provided by the KSA here: [http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA%20\\_001\\_E\\_%20Telecom%20Act%20English.pdf](http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA%20_001_E_%20Telecom%20Act%20English.pdf)

An unofficial translation of the Telecom Act Bylaws is provided by the KSA here: [http://www.citc.gov.sa/English/RulesandSystems/Bylaws/Documents/LA\\_005\\_%20E\\_Telecom%20Act%20Bylaws.pdf](http://www.citc.gov.sa/English/RulesandSystems/Bylaws/Documents/LA_005_%20E_Telecom%20Act%20Bylaws.pdf)

An official translation of the Anti-Cyber-Crime Law is available here: [http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA\\_004\\_%20E\\_%20Anti-Cyber%20Crime%20Law.pdf](http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf)

In addition, Shari’ah or Islamic law principles create a tort for wrongful disclosure of a person’s private information.

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Council of Ministers of KSA.

2.2 **Registration.** Under Article 18 of the Telecommunications Act, entities providing telecommunication service must register with the government. The Anti-Cyber Crime Law does not have a registration requirement.

## 3. Protected Personal Data

3.1 **Data** is defined in Article 1.4 of the Anti-Cyber Crime Law as information, commands, messages, voices, or images which are prepared or have been prepared for use in computers. This includes data that can be saved, processed, transmitted, or constructed by computers (e.g., numbers, letters, codes.)

There is no corresponding specific definition of data or personal data in the KSA's Telecommunications Act. However, "telecommunications" are defined to include information transmitted over the Internet.

#### **4. Data Collection and Processing**

Under Article 37.7 of the Telecommunications Act, Internet service providers and telecommunications companies are prohibited from intercepting any data carried across their public systems unless otherwise allowed by law.

Under Articles 3 and 5 of the Anti-Cyber Crime Law, unauthorized access to data is a crime where the data is modified, deleted, or destroyed.

#### **5. Data Transfer**

Under Article 37.13 of the Telecommunications Act, disclosure of data is a violation unless it is in the course of duty. This applies to operators, those who own the data, as well as third parties.

Under the *Anti-Cyber Crime Law*, there is no specific provision on data sharing or transfer, but if such sharing was subsequent to unauthorized access to the data such an act would likely be a violation.

#### **6. Data Security**

N/A

#### **7. Breach Notification**

N/A

#### **8. Other Considerations**

N/A

#### **9. Enforcement and Penalties**

Under the Telecommunications Act, violations may result in penalties of up to SAR 5,000,000.

Under the Anti-Cyber Crime Law, unlawful access to data that jeopardizes internal or external security or the national economy may result in up to 10 years in prison and fines up to SAR 5,000,000.

## 1. Applicable Law

On January 2, 2013, Singapore's Personal Data Protection Act 2012 ("PDPA") went into effect, the same day Singapore's [Personal Data Protection Commission \(PDPC\)](#) was established; the entirety of PDPA came into effect on July 2, 2014. The "purpose" of the law "is to govern the collection, use and disclosure of personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances." The official text of the PDPA is provided by the Singapore Parliament here:

<http://www.parliament.gov.sg/sites/default/files/Personal%20Data%20Protection%20Bill%202012-2012.pdf>

The PDPC followed-up the implementation of the PDPA with a further guidance note on September 24, 2013 which, among other topics, gave direction to organizations regarding notification requirements for the collection, use, or disclosure of personal data [as well as the anonymization of personal data](#). This guidance outlined the use of 'cookies' for internet user's online activity, distinguishing in part between active consent on one hand, and "[the mere failure of an individual to actively manage his browser settings](#)" on the other.

## 2. Data Protection Authority

2.1 The PDPA provides for the creation of a Data Protection Commission ("DPC") of no fewer than three, but not more than seven members to oversee the implementation of the PDPA. The DPC has authority, among other things, to:

- promote awareness of data protection in Singapore;
- provide consulting, advisory and other similar services relating to data protection;
- advise the Singapore government on data protection matters and to represent the Singapore government internationally on data protection matters;
- issue guidelines regarding data protection and the PDPA;
- attempt to remedy non-compliance with the PDPA;
- review compliances of violations of the PDPA and to initiate investigations regarding the same; and
- impose financial penalties for violations of the PDPA of up to S\$1 million.

## 3. Protected Personal Data

The PDPA applies to both electronic and non-electronic data.

3.1 **Personal data** is data, whether true or not, about an individual who can be identified from that data or other data to which the organization likely has access.



3.2 **Sensitive data** is not specifically defined by the PDPA. There is a provision preventing the disclosure of personal data about an individual for archival or historical purposes without his/her consent if a reasonable person would consider the personal data to be too sensitive to the individual to be disclosed at the proposed time.

#### 4. Data Collection and Processing

4.1 Processing is the carrying out of any operation or set of operations in relation to personal data, and includes any of the following:

- recording;
- holding;
- organization, adaptation or alteration;
- retrieval;
- combination;
- transmission; or
- erasure or destruction.

4.2 Under the PDPA, an organization shall not, on or after the date that the PDPA goes into effect, collect, use or disclose personal data about an individual unless:

- the individual gives, or is deemed to give, his consent; or
- the collection, use or disclosure, is required or authorized by law.

4.3 There are certain limited exceptions to obtaining consent as outlined in the PDPA.

4.4 Consent under the PDPA may be express or deemed. An individual is deemed to consent if the individual voluntarily provides the personal data to an organization for its collection, use or disclosure and it is reasonable that the individual would voluntarily provide the data.

4.5 An individual who gives consent may, on giving reasonable notice to the organization, withdraw that consent and, once withdrawn, the organization is required to stop processing the individual's personal data, unless otherwise allowed under the Act or other law.

4.6 Subject to the PDPA, an organization may collect, use or disclose personal data only for purposes:

- that a reasonable person would consider appropriate in the circumstances; and
- that the organization informs the individual under section 20 of the Act, if applicable.

4.7 Special Considerations Regarding Employee Data:

- The PDPA extends to the employment context and personal data related to employees, including potential and former employees, and most if not

all employers are covered under the PDPA (even if indirectly), though consent is not always required. The PDPA defines “employee” to include volunteers, and the definition of “employment” includes working under an “unpaid volunteer work relationship.”

## **5. Data Transfer**

- 5.1 Under the PDPA, an organization shall have the same obligation with regard to personal data processed on its behalf by a data intermediary as if the personal data were processed by the organization itself.
- 5.2 When transferring personal data outside of Singapore, organizations must provide a standard of protection that is comparable to that of the PDPA. Organizations seeking to transfer personal data outside of Singapore may apply to the DPC for an exemption from this requirement.

## **6. Data Security**

- 6.1 An organization must protect personal data in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.
- 6.2 In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate under the circumstances.
- 6.3 Organizations subject to the PDPA must designate one or more individuals to be responsible for ensuring compliance with the PDPA.
- 6.4 Organizations subject to the PDPA shall:
  - develop and implement policies and practices necessary for the organization to meet its obligations under the PDPA;
  - develop a process to receive and response to complaints concerning compliance with the PDPA;
  - communicate to its employees information about the organization’s data protection policies and practices; and
  - make information available on request about:
    - the organization’s data protection policies and practices; and
    - the organization’s complaint process.
- 6.5 An organization must make a reasonable effort to ensure that personal data collected by or on behalf of the organization is accurate and complete, if the personal data:
  - is likely to be used by the organization to make a decision that affects the individual to whom the personal data relates; or
  - is likely to be disclosed by the organization to another organization.
- 6.6 An organization must stop retaining its documents containing personal data or render the documents anonymous as soon as it is reasonable to assume that the

purpose for which the data was collected is no longer being served by its retention and the retention is no longer necessary for legal or business purposes.

## **7. Breach Notification**

7.1 The PDPA does not provide a specific breach notification requirement.

## **8. Other Considerations**

8.1 The PDPA applies to all organizations except that Parts III to VI do not impose any obligations on public agencies (defined to include the Singapore government and any statutory body and tribunals appointed under the law) and certain specific other exceptions as outlined in the PDPA. "Organization" is defined broadly to include "any individual, company, association or body of persons, corporate or unincorporated," subject to certain limited exceptions as outlined by the PDPA.

8.2 The PDPA established a Do Not Call ("DNC") Register to allow individuals to opt-out of receiving marketing messages by registering their Singapore phone numbers. It is anticipated that individuals may begin signing up for the DNC Registry in early 2014.<sup>13</sup>

## **9. Enforcement & Penalties**

9.1 Under the PDPA, the DPC is responsible for investigation and enforcement of compliance with the PDPA. The DPC may initiate an investigation into non-compliance on its own volition or upon receiving a complaint. The DPC may, if it believes an organization is not complying with the PDPA, give the organization such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision. This could include directing the organization to:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- comply with any other direction of the DPC per the PDPA; or
- pay a financial penalty not to exceed S\$1 million.

9.2 Certain offenses under the PDPA committed with the consent, connivance, or neglect of an organization's officer may result in liability for the officer as well as the corporation.

9.3 Individuals who suffer loss or damage for violations of the PDPA pursuant to the PDPA have the right to initiate a private cause of action for relief in a court, subject to certain exceptions as provided in the PDPA.

9.4 Organizations may appeal certain decisions made by the DPC pursuant to the PDPA.

---

<sup>13</sup> <http://www.futuregov.asia/articles/2012/oct/17/singapore-passes-first-personal-data-protection-bi/>

## 1. Applicable Law

- 1.1 On March 29, 2011, South Korea approved the comprehensive Protection of Personal Data Act (“PIPA”). PIPA went into effect on September 30, 2011. The South Korean government provided a grace period for companies to comply with the provisions of the new law, which came to an end on March 31, 2012. PIPA was amended on August 6, 2013; the amendments came into force on August 7, 2014. The application of PIPA is not limited to South Korean borders; if an actor violates PIPA, causing damage to a South Korean citizen or company, South Korea considers that actor subject to South Korean law.

The official texts of PIPA can be found here:

<http://www.law.go.kr/lsInfoP.do?lsiSeq=111327#0000>.

An Unofficial English Translation of PIPA as amended is available here:

[http://koreanlii.or.kr/w/images/a/a3/PIPAAct\\_1308en.pdf](http://koreanlii.or.kr/w/images/a/a3/PIPAAct_1308en.pdf)

The official text of PIPA’s Enforcement Decree is available here:

<http://www.law.go.kr/lsInfoP.do?lsiSeq=117349#0000>.

An Unofficial English Translation is available here:

[http://koreanlii.or.kr/w/images/d/d7/DPAct\\_EnforceDecree.pdf](http://koreanlii.or.kr/w/images/d/d7/DPAct_EnforceDecree.pdf)<sup>14</sup>

- 1.2 In addition to the comprehensive legislation, South Korea also has industry specific legislation, which remains good law to the extent it is not superseded by PIPA. For instance, the Act on Promotion of Information and Communication Network Utilization and Information Protection (“IT Network Act”), which regulates collection and use of personal information in telecommunications business; the Act on Real Name Financial Transactions and Guarantee of Secrecy (“ARNFTGS”), which applies to information obtained by the financial industry; the Use and Protection of Credit Information Act; and the Protection of Use of Location Information Act.

An English translation of the IT Network Act Can be found here:

<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf>

An English Translation of the ARNFTGS can be found here:

[http://www.imolin.org/doc/amlid/korea\\_real\\_name\\_financial\\_transaction\\_act.pdf](http://www.imolin.org/doc/amlid/korea_real_name_financial_transaction_act.pdf)

- 1.3 Article 16 of PIPA was amended on August 6, 2013 to incorporate an affirmative obligation on the part of a personal information processor, requiring notification to data subjects that data subjects may deny consent for the collection of any personal information other than for any purposes under Article 15(1). These August 6, 2013 amendments will come into force on August 6, 2014.

---

<sup>14</sup> This translation was created by Prof. Whon-il Park.

## 2. Data Protection Authority and Registration Requirements

### 2.1 Authorities

Under PIPA: The Minister of Public Administration and Security (“MOPAS”).

Under the IT Network Act: The Korean Communications Commissions (“KCC”).

### 2.2 Registration requirements

Under PIPA for public institutions:

- name of data subjects;
- basis and purposes of the collection of personal information;
- specific items of personal information collected;
- method of processing the personal information;
- period to retain the personal information;
- name of the person who receives the personal information generally or repeatedly; and
- other matters as listed by the Presidential decree.

## 3. Protected Personal Information

### 3.1 Under PIPA:

**Personal information** is defined as the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, *etc.* (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information). This includes any collection of South Korean Resident Registration Numbers (“RRNs”).

**Sensitive data** includes any of the following: ideology, belief, admission/exit to and from trade unions or political parties, political mindset, health, sexual life, and other personal information which is likely to do harm to the privacy of data subjects.

### 3.2 Under IT Network Act:

**Personal information** is information pertaining to a living person, which contains information identifying a specific person with a name, a national identification number or similar information in a form of code, letter voice, sound, image or any other form (including information which, if not by itself, makes it possible to identify any specific individual if combined with other information).

## 4. Data Collection and Processing under PIPA and IT Network Act

### 4.1 Under PIPA and the IT Network Act, every data handler and/or service provider must designate a data protection officer.

- 4.2 As a general rule, data can only be collected after notifying the data subject and obtaining consent.
- 4.3 Under PIPA, consent can be obtained after provided the following information to the data subject:
- the purpose of the collection and the use of personal information;
  - particulars of the personal information to be collected;
  - the time frame when personal information is retained and used; and
  - the fact that data subjects can deny consent and notice of any consequences from the denial of consent.
- 4.4 Under the IT Network Act, consent can be obtained after providing the following information to the IT user:
- the name, department, position, telephone number, and other contact information of a person in charge of administering the personal information;
  - the purpose of the collection and the use of personal information;
  - the particulars of the personal information to be provided to a third person;
  - the rights of the user and his legal representative and the method of exercising this right; and
  - other matters stipulated by the Presidential Decree.
- 4.5 If a data processor intends to process “sensitive data,” he or she needs separate consent from the data subject under PIPA.
- 4.6 Under August 6, 2013 amendments to Article 24 of PIPA, ISPs are prohibited from processing RRNs except in a few limited circumstances.
- 4.7 If the personal information relates to a person under 14, under PIPA and the IT Network the consent of the child’s parent or guardian must be obtained.
- 4.8 Under PIPA, exceptions to the requirement of consent prior to the collection of data are as follows:
- special provisions exist in laws or it is necessary to observe legal obligations;
  - where it is unavoidable so that the public institution may carry out work as required by law;
  - where it is unavoidably necessary to execute and perform a contract with the data subjects;
  - where it deems necessary explicitly for the protection, from impending danger, of life, body or economic profits of the data subject or a third party in certain situations; or
  - where it is necessary to attain the justifiable interest of the personal information processor, which is explicitly superior to that of data subjects.

- 4.9 Under the IT Network Act, exceptions to the requirement of consent prior to the processing of personal information are as follows:
- the information is necessary in performing a contract communications services;
  - if necessary to settle payment for IT services provided; or
  - where a specific provision exists in law.
- 4.10 Under ARNFTGS, employees of financial institutions shall not provide or reveal information concerning the contents of financial transactions to other persons unless they receive a request or consent in writing.

## 5. Data Transfer

- 5.1 Data cannot be processed by or shared with a third party unless:
- consent from the data subject is obtained;
  - under PIPA, the information is shared under the circumstances permitting the collection of data under the enumerated subparagraphs; or
  - under the IT Network Act:
    - where it is necessary to charge fees for information and communications service provision;
    - if such personal information is necessary to compile statistics, conduct academic research, or conduct a market survey, under certain circumstances; or
    - where special provisions exist in other Acts.
- 5.2 Data Sharing
- Under PIPA, in the event of a transfer of business in whole or in part, or merger, *etc.*, the personal information processor shall notify the data subject of the following as stated in the Presidential Decree:
    - the fact that the personal information will be transferred;
    - the name, address, telephone number and other contact information of the recipient of the personal information; and
    - the method and procedure to withdraw the consent.

## 6. Data Security

- 6.1 General rule: the personal information processor shall take steps to ensure the protection of personal information.
- 6.2 The personal information processor must establish a privacy policy.
- 6.3 The personal information processor shall designate a privacy officer to be in charge of the following:
- establish and implement the data protection plan;
  - to make regular survey of the actual state and practices of personal information processing and to improve shortcomings;

- to address grievances;
- to set up an internal control system to prevent disclosure of personal information;
- to prepare and implement data protection education programs;
- to protect, control and manage the personal information files; and
- other functions as stated by the Presidential Decree.

## 7. Breach Notification

7.1 Under PIPA, the personal information processor shall notify aggrieved data subjects without delay when it becomes known that personal information is leaked.

7.2 Under PIPA, notice shall include:

- the kind of personal information leaked;
- when and how personal information was leaked;
- any information on how the data subject can minimize probable damage due to the leakage;
- countermeasures of the personal information processor and remedial procedure; and
- contact information for the personal information processor so data subjects can report sufferings.

7.3 Under PIPA Regulatory Notice: If it is a large scale breach exceeding 10,000 data subjects, the personal information processor must report the result of measures taken to the Minister of Public Administration and Security, the Korea Internet & Security Agency or the National Information Security Agency.

7.4 Under the IT Network Act, the service provider must immediately report a breach to the Korean Communications Commissions (“KCC”) or the Korean Internet & Security Agency (“KISA”) and analyze the cause of the breach and prevent damage.

## 8. Enforcement & Penalties

8.1 Under PIPA and the IT Network Act, the relevant authorities may request reports on the handling of personal information and then issue orders or recommendations if they discover non-compliance.

- Non-compliance can result in fines, imprisonment or both.

8.2 The Personal Information Dispute Mediation Committee was established to mediate any dispute over personal information.



## 1. Applicable Law

In November of 1999, the Special Data Protection Act 1999 (known as the “LOPD” in Spain), formally implemented the EU Data Protection Directive 95/46/EC. Prior to its enactment, Spain had a Data Protection Act (known as the “LORTAD” in Spain), which was already consistent with the EU Directive. The last amendment to Spain’s data protection law was in 2011.

[http://www.agpd.es/portaleswebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley\\_Organica\\_15-1999\\_de\\_13\\_de\\_diciembre\\_de\\_Proteccion\\_de\\_Datos\\_Consolidado.pdf](http://www.agpd.es/portaleswebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf)

## 2. Data Protection Authority and Registration Requirements

- 2.1 The Spanish Data Protection Commissioner’s Office (“AEPD”) enforces Spain’s data protection law. Regional commissioners also enforce the law, but their primary responsibility concerns data protection issues surrounding the regional public authorities.
- 2.2 Spain does not maintain a registry of data controllers or data processing activities. Instead, the AEPD maintains a registry of databases containing personal data.

## 3. Protected Personal Data

- 3.1 **Personal data** is defined as any information concerning identified or identifiable natural persons.
- 3.2 **Sensitive personal data** is not defined in the Act. Instead, “Data with special protection” includes personal data which reveals the ideology, trade union membership, religion, beliefs, racial origin, health or sex life. Each category of personal data is afforded its own level of protection.

## 4. Data Collection and Processing

- 4.1 In order to collect and process data, any of the following conditions may be met:
  - unambiguous consent from the data subject;
  - data are collected for the exercise of the functions proper to public administrations within the scope of their responsibilities;
  - data needs to be processed in order to carry out a contractual obligation or preliminary contract for a business, employment, or administrative relationship, and are necessary for its maintenance or fulfillment;
  - the purpose of processing the data is to protect a vital interest of the data subject; or
  - data is collected from public sources and the processing is necessary to satisfy a legitimate interest pursued by the controller or that of the third party to whom the data are communicated, provided that the rights of the data subject are preserved.

- 4.2 For the processing of sensitive personal data, a separate list of more stringent conditions must be satisfied.

## 5. Data Transfer

- 5.1 Personal data may be transferred to third parties when:

- the prior consent is obtained from the subject;
- the transfer is endorsed by law;
- the data is collected from public sources;
- the transfer to the third party is essential to a contract, to which the data subject is a party;
- the communication is for certain government bodies;
- the transfer is between public administrations and concerns the retrospective processing of the data for historical, statistical or scientific purposes; or
- the transfer is needed to resolve an emergency which requires access to a file or for conducting epidemiological studies.

- 5.2 International Data Transfers

Transfer of personal data is allowed within the EU/European Economic Area (EEA) without further requirements.

- 5.3 Transfers of data outside the EEA is not permitted unless:

- the international transfer of personal data is the result of applying treaties or agreements to which Spain is a party;
- the transfer serves the purposes of offering or requesting international judicial aid;
- the transfer is necessary for medical prevention or diagnosis, the provision of health aid or medical treatment, or the management of health services;
- the transfer of data is related to money transfers in accordance with the relevant legislation;
- the data subject has given unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller (or the adoption of pre-contractual measures taken at the data subject's request);
- the transfer is necessary for the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject, between the controller and a third party;
- the transfer is necessary or legally required to safeguard a public interest;
- the transfer is necessary for the recognition, exercise or defense of a right in legal proceedings;
- the transfer takes place at the request of a person with a legitimate interest, from a public register, and the request complies with the purpose of the register; or
- the transfer is to a country that the European Commission has declared ensures an adequate level of protection. Transfers to the United States

may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework.

Transfer to a country that does not meet any of the above standards may still be permitted with prior authorization from the Director of the Data Protection Agency if the Director deems adequate guarantees to have been obtained. Here, the use of the binding corporate rules framework or EU model contractual clauses would be relevant.

## **6. Data Security**

Those who collect, process and control personal data must implement appropriate technical and organizational safeguards to prevent the unauthorized or unlawful access or processing of personal data and the accidental loss or destruction of or damage to personal data. The level of security safeguards implemented depends on the nature of the personal data at issue.

## **7. Breach Notification**

At the time of publication, there is no mandatory requirement to report data security breaches or losses of personal data to the AEPD or to affected individuals.

## **8. Penalties**

Fines generally range from Ptas 100,000 to Ptas 10,000,000 for minor infringements, Ptas 10,000,000 to Ptas 50,000,000 for serious infringements, and Ptas 50,000,000 to 100,000,000 for very serious infringements.

## 1. Applicable Law

In 1995, Taiwan passed the Computer-Processed Personal Data Protection Law (“CPPDP”) and its associated rules (“Rules”). In 2010, the CPPDP was amended and retitled the Personal Information Protection Act (“PIPA”). On October 1, 2012, this act came into effect. Further amendments were proposed in August, 2012, but those amendments have not been passed by the legislature.

The official version of the Act, in Mandarin, is available here:  
<http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021>.

The government has provided an English translation, available here:  
<http://law.moj.gov.tw/eng/LawClass/LawAll.aspx?PCCode=I0050021>.

## 2. Data Protection Authority and Registration Requirements

2.1 **Authority.** The Ministry of Justice is the responsible enforcement and rule promulgating authority for PIPA.

2.2 **Registration.** PIPA itself does not require registration.

## 3. Protected Personal Data

3.1 **Personal information** is defined as the name, date of birth, I.D. card number, passport number, characteristics, finger print, marital status, family, education, profession, health examination, medical record, financial condition, and social activities and other information which may be used to identify a natural person, both directly and indirectly.

3.2 **Personal information file** is defined as a collection of personal information built to allow information retrieval and management by automatic or non-automatic measures.

3.3 **Sensitive personal information** is not specifically defined in PIPA. However, there are special conditions under the Act for personal information of medical treatment, genetic information, sexual life, health examination and criminal records.

## 4. Data Collection and Processing

4.1 **Government agencies.** Government agencies are not allowed to collect and process personal data unless there is a specific purpose and:

- it is within the scope of job functions as provided in laws and regulations;
- with the written consent of a concerned party; and
- there is no potential harm to be done to the rights and interests of a concerned party.

The government should use the personal information in accordance with the scope of its job functions and in compliance with the specific purpose of collection. However, the information may be used outside the scope:

- where allowed by law;
- for national security or to promote public interests;
- to prevent harm on the life, body, freedom or property of the person;
- to prevent harm on the rights and interests of other people;
- where it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively, under certain circumstances;
- where such use may benefit the person; or
- where written consent has been given.

4.2 **Non-government agencies.** Non-government agencies are not allowed to collect or process personal information, unless there is a specific purpose and:

- where allowed by law;
- where there is a contract or quasi-contract between the person and the agency;
- where the person has disclosed such information by himself or when the information has been legally publicized;
- where it is necessary for public interests on statistics or the purpose of academic research conducted by a research institution, under certain circumstances;
- where written consent has been given;
- where the public interest is implicated; or
- where the personal information is obtained from publicly available resources, except in certain circumstances.

4.3 The non-government agency should use the personal information in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside the scope:

- where allowed by law;
- to promote public interests;
- to prevent harm on the life, body, freedom or property of the person;
- to prevent harm on the rights and interests of other people;
- when necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively, under certain circumstances; or
- where written consent has been given.

## 5. Data Transfer.

Non-public institutions are subject to restrictions on the transfer of personal data where:

- it involves major national interests;
- transfer of data is restricted by treaty or agreement;

- the receiving country does not have proper laws and/or ordinances to adequately protect personal data and it is possible that a party may be injured as a result; or
- the transfer is to avoid the laws of Taiwan.

## 6. Data Security

- 6.1 A government agency maintaining a personal data file must designate staff to take charge of maintenance of safety so as to protect personal data from burglary, alteration, destruction, damage, or disclosure.
- 6.2 The non-government agency which keeps personal information files should adopt proper security measures to protect them.

## 7. Breach Notification

If the personal information is stolen, disclosed, altered, or infringed in other ways due to the violation of this law, the government agency or non-government agency should notify the subject after an inspection.

## 8. Other Considerations

- 8.1 PIPA allows owners of personal data to make the following on a holder of their data: (i) a request for review, (ii) a request for duplicates, (iii) a request for supplements or amendments, (iv) a request to cease collection of computerized processing and use; or (v) a request for deletion. These rights should be exercised and should not be waived in advance or limited by a specific agreement.

## 9. Enforcement and Penalties

- 9.1 **Damages.** Government agencies that violate PIPA are liable for damages. The total amount of damages awarded must be at least NT\$500 and may not be more than NT\$20,000 for each event to each person unless actual damages are higher. Where there are multiple violations from a single event, damages are capped at NT\$200,000,000. These are subject to certain exceptions.
- 9.2 Non-government agencies may be liable for the same schedule of damages if the violation was caused by illegal collection, processing and using of personal information, or other ways of infringement due to violation of PIPA.
- 9.3 **Penalties.** Criminal penalties exist and impose a maximum term of imprisonment of two years and a fine of not more than NT\$200,000.

---

# Trinidad and Tobago

## 1. Applicable Law

In 2011, the Parliament of Trinidad and Tobago introduced the Data Protection Act 2011 (the “Act”). The Act was enacted in January 2012.

The Parliament has provided a link to the text of the Act here:

<http://www.ttparliament.org/legislations/a2011-13.pdf>

## 2. Data Protection Authority and Registration Requirements

2.1 Office of the Information Commissioner (“OIC”).

2.2 The Commissioner has the responsibility of monitoring the administration of the Act in order to ensure its purposes are achieved. The Commissioner may, among other things, conduct audits and investigations, may advise on privacy protections, authorize the collection of personal information, and publish guidelines regarding compliance with the Act. The Act provides for the establishment of a “mandatory code of conduct.”

2.3 There are no requirements for registration under the Act.

## 3. Protected Personal Data

3.1 **Personal data** is any information about an identifiable individual that is recorded in any form. Personal information includes:

- information relating to the race, nationality or ethnic origin, religion, age or marital status of the individual;
- information relating to the education or medical, criminal or employment history of the individual, or information relating to the financial transactions in which the individual has been involved, or which refers to the individual;
- any identifying number, symbol or other particular designed to identify the individual;
- the address and telephone contact number of the individual;
- 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;
- any correspondence sent to an establishment by the individual that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence which would reveal the contents of the original correspondence;
- the view and opinions of any other person about the individual; and
- the fingerprints, DNA, blood type or the biometric characteristics of the individual.

3.2 **Sensitive personal information** includes information pertaining to:

- 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; and
- criminal or financial records.

#### 4. Data Collection and Processing

4.1 The Act provides “general privacy principles,” which must be followed by all entities:

- an entity that handles, stores or processes personal information must be responsible for the personal information under its control;
- the purpose for the collection shall be identified before or at the time of collection;
- knowledge or consent of the individual is required for collection, use or disclosure;
- personal information shall be legally collected and may only be used for the purpose identified;
- personal information can also only be retained for as long as is necessary, and may not be disclosed for purposes other than for the purpose collected, unless prior consent has been obtained;
- personal information collected must be accurate, complete, and up to date as is necessary for the purpose of collection;
- personal information must also be protected by appropriate safeguards and with regard to the sensitivity of the information;
- organizations must make available to individuals documents regarding their policies and practices related to the management of personal information, except where otherwise provided by written law;
- organizations 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; and
- the data subject has the ability to challenge the organization’s compliance with the above principles and receive timely and appropriate engagement from the organization.

4.2 Sensitive personal information may not be processed without consent, except under the following circumstances:

- it may be processed by a health care professional or an employee or agent of a health care body where necessary for preventative medicine and the protection of public health, medical diagnosis, health care and treatment, and the management of health and hospital care services;
- where it has been made public by the person to whom such information relates;
- for research and statistical purposes in accordance with the Act;
- in the interest of law enforcement and national security;
- for the purposes of determining access to social services; or
- where the disclosure is required by written law.



- 4.3 The Act provides a lengthy set of data collection, processing, and sharing regulations applicable specifically to public bodies, which includes corporations controlled by or established for the State or Government, some more and some less stringent than regulations provides for non-public entities.
- 4.4 Special Considerations Regarding Employee Data
- The Act does not protect the following personal information for employees or officials of a public body:
    - the fact that the individual is or has been an employee or official of a public body;
    - the title, business address and business telephone number of the individual;
    - the name of the individual on a document prepared by the individual in the course of employment; or
    - the professional opinions or views of the individual given in the course of employment.

## **5. Data Transfer**

Personal information disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under the Act must exist in the jurisdiction receiving the personal information.

- 5.1 For any collection and/or transfer of personal information outside of the country, the individual must be notified of the purpose for which the information is being collected once that purpose is known to the organization; and the identity of the person requesting the information and the relevant public body with responsibility for data protection in the other jurisdiction.
- 5.2 The individual must consent to the release of personal information outside of the country.
- The above two provisions do not apply in certain circumstances.
- 5.3 Also, upon a referral OIC shall make a determination as to whether the other jurisdiction has or does not have comparable safeguards as provided by this Act, and inform the organization accordingly.

## **6. Data Security**

- 6.1 While the Act does not specify the type of security measures to adopt and implement for the safeguarding of personal data, the Act does permit the OIC and/or an appropriate government regulator of an industry (with approval from the OIC) to develop a mandatory or voluntary code of conduct for an industry, economic sector, or activity.

## **7. Breach Notification**

- 7.1 At the time of publication, there is no mandatory requirement to report data security breach incidents under the Act.

## **8. Other Considerations**

- 8.1 The Act's regulations pertaining to nonpublic entities apply to any person who (a) collects, retains, manages, uses, processes or stores personal information in Trinidad and Tobago; (b) collects personal information from individuals in Trinidad and Tobago; or (c) uses an intermediary or telecommunications service provider located in Trinidad and Tobago to provide a service in furtherance of (a) or (b).
- 8.2 The Act provides individuals whose personal information is stored in an organization which is subject to a mandatory code of conduct a right of access to their personal information. An individual can send a request requiring the data processor to tell them about the personal information it holds about them and to provide them with access to that information.

## **9. Enforcement & Penalties**

- 9.1 The following constitute offenses under the Act:
- willful obstruction of an OIC investigation;
  - request for access to or correction of personal information under false pretenses;
  - willfully making a false statement to mislead or attempting to mislead the OIC in the performance of his/her functions under the Act;
  - failure to comply with an order of OIC;
  - violation of whistle-blowing provisions;
  - failure to comply with a mandatory code of conduct;
  - willful disclosure of personal information in contravention of the Act;
  - collection, storage, or disposal of personal information in contravention of the Act; or
  - committing a breach of the confidentiality obligations established by the Act
- 9.2 A person who commits an offense under this Act is liable upon summary conviction for a fine or not more than TT\$50,000 or for imprisonment for a term of three years. Where a person is found liable upon conviction on indictment, a fine may be issued for no more than TT\$100,000 or imprisonment for a term of not more than five years.
- 9.3 When a corporate body which commits an offense under this Act is liable upon summary conviction, a fine may be issued of TT\$250,000. Where the offense is committed by a corporate body, and upon conviction on indictment, a fine may be issued of TT\$500,000. Further, any officer, director or agent of a corporation who directs, authorizes, assents to, or participates in the commission of an offense under the Act is a party to and commits the offense and is liable.

## 1. Applicable Law

In 2013, the Ukrainian parliament amended Ukraine's data privacy law. These amendments entered into force on January 1, 2014 (the "Amendments"<sup>15</sup>). This legislation amends the 2011 Law of the Ukraine on Personal Data Protection ("Law"). Significantly, the Amendments change the role of the current State Service of Ukraine on Personal Data Protection, transferring its functions to the Human Rights Commissioner of the Parliament of Ukraine ("Ombudsman").

The overall shift to Ombudsman oversight and the creation of an independent authority for data protection issues brings Ukraine closer to compliance with European data protection standards, even though Ukraine is not a member state. Further changes incorporate the designation of "High Risk Data," the processing of which carries requirements of notification to the Ombudsman, and consent requirements for the transfer of individuals' data, with failures and breaches subject to civil and criminal penalties, including imprisonment of up to 5 years.

An unofficial translation of the 2011 Law of the Ukraine on Personal Data protection is provided by the Ukrainian government here: <http://zpd.gov.ua/dszpd/en/publish/article/39178>.

The amended text is available in the original Ukrainian at the following website: <http://zakon4.rada.gov.ua/laws/show/383-vii>.

In the Ukraine, there are also various data protection issues that are regulated by other legislation developed to enforce the data protection law.

## 2. Data Protection Authority and Registration Requirements

2.1 Under the Amendments, the Ombudsman is the entity entrusted with personal data protection. Compliance with the data protection legislation is enforced by the authorized state body on matters of personal data protection and other state bodies. The Commissioner for Human Rights (Ombudsman) exercises parliamentary control to make sure that people's rights are respected with regard to personal data.<sup>16</sup> The Amendments place significant data protection responsibility with the Ombudsman, including:

- Hearing complaints;
- Conducting inspections and privacy audits;
- Adopting regulations as stipulated by the Amendments; and
- Submitting proposals for amendments to the data protection regime.

2.2 Under the previous data protection regime, all data personal data databases were required to be registered with the State Register. The Amendments abolished this registration procedure and instead imposes a new notification procedure. Data controllers must notify the Ombudsman of personal data processing only in cases where such processing subjects data to high risk. The

<sup>15</sup> On Amending Certain Legislative Acts of Ukraine Regarding Improving the System of Personal Data Protection" No. 383-VII, dated July 3, 2013.

<sup>16</sup> <http://first-ombudsman.org.ua/en/zahist-personalni-dani-z.html>

criteria for what puts personal data at high risk has not been clearly set out in the law. It may be that further implementing regulation from the Ombudsman will define this.

### 3. Protected Personal Data

- 3.1 **Personal data** is any information or collection of information about a person who is identified or may be identified.
- 3.2 **Sensitive personal data** is not defined in the Act, although special protection is provided to information that reveals racial or ethnic origins; political views, philosophical or religious opinions; political party or trade-union membership; criminal charges or convictions; health; sexual life, and biometric or genetic data.

### 4. Data Collection and Processing

- 4.1 Ukraine's data protection law establishes requirements for the collection and processing of personal data. Within 10 working days of the collection of the data, an individual must be informed of:
- the identification of the owner of the database;
  - a description of the data collected;
  - the individual's privacy rights;
  - the purpose of the data collection; and
  - the identification of parties to whom the data is transferred.
- 4.2 For the collection of sensitive personal data, such collection and use is generally prohibited except in limited circumstances.

### 5. Data Transfer

- 5.1 Personal data may be transferred to foreign personal data processors where they ensure a sufficient level of data protection, and the transfer of personal data is for the same purpose for which it was collected.
- Members of the EU and signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are recognized as providing adequate levels of protection.
  - The Ukrainian Cabinet may also determine whether a state provides adequate protection.
- 5.2 Notwithstanding the above, personal data may be transferred to foreign personal data processors where:
- the subject of the transfer provides unambiguous consent;
  - the transfer is necessary for the fulfillment of a contract which benefits the subject of the transfer;
  - the transfer is necessary for the protection of vital interests of the subject;
  - the transfer is necessary for the protection of the public interests or the implementation of legal rights; or

- the data processor provides adequate safeguards that the transfer will not interfere with the subject's private life.

## **6. Data Security**

Data processors shall provide protection from unauthorized processing (including loss, unlawful or accidental destruction) and unauthorized access.

## **7. Breach Notification**

There are no requirements pertaining to notification in the event of a breach incident.

## **8. Penalties**

The Amendments contain an increase in penalties from UAH 17,000 to UAH 34,000. Fines may be accompanied by imprisonment for up to 3 years.

---

# United Arab Emirates

## 1. Applicable Law

The United Arab Emirates (“UAE”) is a federation of seven Emirates, including Dubai and Abu Dhabi, which together make up over two-thirds of the country’s population. There is no specific data privacy legislation that applies to all seven Emirates. However, the following UAE laws contain provisions related to data processing:

- Article 31 of the UAE Constitution of 1971, which guarantees the right to secrecy of communications.
- Federal Law No. 5 of 1985 regarding Civil Transactions, which holds an individual liable for acts causing harm through the unauthorized use of the personal or private information of another.
- Articles 378 and 379 of the UAE Penal Code, setting out the statutory offenses and punishments related to the publication of private matters or the unauthorized disclosure of private information.

The Dubai International Finance Center (“DIFC”) operates as an independent jurisdiction with the authority to promulgate its own laws and regulations. The DIFC’s legislative system is consistent with English Common law.<sup>17</sup> In 2007, the DIFC promulgated Data Protection Law No. 1 of 2007 (“DPL”), based largely on European Union data privacy directives. The Data Protection Law was recently amended, effective December 23, 2012. The official DIFC version of the amended text is available here:

[http://www.difc.ae/sites/default/files/Data%20Protection%20Law%20Amendment%20Law\\_DIFC%20Law%20No.%205%20of%202012%20mark%20up\\_enacted\\_16%20Dec%202012.-v3doc\\_0.pdf](http://www.difc.ae/sites/default/files/Data%20Protection%20Law%20Amendment%20Law_DIFC%20Law%20No.%205%20of%202012%20mark%20up_enacted_16%20Dec%202012.-v3doc_0.pdf)

## 2. Data Protection Authority and Registration Requirements

- 2.1 The DPL and its accompanying regulations are administered by the Commissioner of Data Protection (“Commissioner”), an official appointed by the President of the DIFC.
- 2.2 Data Controllers shall establish and maintain records of any personal data processing operations and shall file a notification with the Commissioner.

## 3. Protected Personal Data

- 3.1 **Personal Data** is defined under the DPL as any data relating to an Identifiable Natural Person.
- 3.2 **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/her biological, physical, biometric, physiological, mental, economic, cultural or social identity.

---

<sup>17</sup> <http://www.difc.ae/discover-difc>

3.3 **Sensitive Personal Data** is 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.

3.4 **Data Subject** is the individual to whom Personal Data relates.

#### 4. **Data Collection and Processing**

4.1 **Data controller** is any person in the DIFC who alone or jointly with others determines the purposes and means of the processing of Personal Data.

4.2 **Process, Processed, Processes, and Processing** means 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.

4.3 **Recipient** is any person to whom Personal Data is disclosed, whether a third party or not; however, authorities which may receive Personal Data in the framework of a particular inquiry shall not be regarded as Recipients.

4.4 General Processing Requirements

Data Controllers shall ensure that Personal Data they Process is:

- Processed fairly, lawfully and securely;
- Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights;
- adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further Processed; and
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal Data was collected or for which they are further Processed.

4.5 Requirement for Legitimate Processing

- Personal Data may only be Processed if:
  - the Data Subject has given his written consent to the Processing of that Personal Data;
  - Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
  - Processing is necessary for compliance with any legal obligation to which the Data Controller is subject;
  - Processing is necessary for the performance of a task carried out in the interests of certain enumerated government bodies; 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.

#### 4.6 Notification to Data Subjects

- Data Controllers must provide Data Subjects whose Personal Data is collected with at least the following information as soon as possible upon commencing the collection :
  - the identity of the Data Controller;
  - the purposes of the Processing for which the Personal Data are intended;
  - any further information insofar as such is necessary, with regard to the circumstances under which the Personal Data are collected, to guarantee fair Processing in respect of the Data Subject, such as:
    - the recipients or categories of recipients of the Personal Data;
    - whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
    - the existence of the right of access to and the right to rectify the Personal Data;
    - whether the Personal Data will be used for direct marketing purposes; and
    - whether the Personal Data will be Processed for specified purposes.

#### 4.7 Processing of Sensitive Personal Data

- Sensitive Personal Data cannot be Processed unless:
  - the Data Subject has given his written consent;
  - Processing is necessary for the Data Controller to carry out his obligations and specific rights;
  - 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;
  - Processing is carried out by a foundation, association, or any other non-profit in the course of its legitimate activities, under certain conditions;
  - Processing relates to Personal Data that the Data Subject has made public, or is necessary for the establishment, exercise or defense of legal claims;
  - Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;
  - Processing is necessary to uphold the legitimate interests of the Data Controller recognized in the international financial markets under certain circumstances;
  - 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;



- Processing is required for medical purposes, under certain circumstances;
- Processing is required for protecting members of the public against certain conduct; or
- Processing authorized in writing by the Commissioner.

## **5. Data Sharing and Data Transfer**

### **5.1 Adequate Protection Required for transfers out of the DIFC**

- A transfer of Personal Data to a Recipient located in a jurisdiction outside the DIFC is prohibited unless an adequate level of protection for that Personal Data is ensured in that jurisdiction.
- A jurisdiction has an adequate level of protection if it is listed as an acceptable jurisdiction under the Regulations promulgated by the Commissioner or if the Commissioner approves the transfer.

### **5.2 Exception: a transfer outside the DIFC to a Recipient who is not subject to an adequate level of protection is permissible if:**

- the Data Subject has given written consent to the transfer;
- the Commissioner grants specific permission and the Data Controller applies adequate safeguards to protect the Personal Data;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a Third Party;
- the transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defense of legal claims;
- the transfer is necessary to protect the vital interests of the Data;
- The transfer is made from a register which is intended to provided information to the public, under certain circumstances;
- the 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;
- the transfer is necessary to uphold the legitimate interests of the Data Controller recognized in the international financial markets, under certain circumstances; or
- the 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 apply to a Data Controller.

## **6. Data Security**

- 6.1 The Data Controller shall implement appropriate technical and organizational measures to protect Personal Data against willful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing, in particular with

regard to Sensitive Personal Data or where adequate protections do not exist in foreign countries.

- 6.2 The security measures must ensure a level of security appropriate to the risks associated with the Processing activity and the nature of the Personal Data (with due consideration for cost).
- 6.3 When Processing is carried out by the Data Collector's delegate or affiliate, the Data Collector must choose a Data Processor providing sufficient guarantees regarding the technical security measures governing the Processing and shall ensure compliance with those measures.

## **7. Breach Notification**

- 7.1 The DPL does not impose a duty on Data Controllers to notify Data Subjects of a breach of their Personal Data.
- 7.2 However, in the event of an unauthorized intrusion, either physical, electronic or otherwise, to any Personal Data database, the Data Controller or the Data Processor carrying out the Data Controller's function at the time of the intrusion, shall inform the Commissioner of the incident as soon as reasonably practicable.

## **8. Other Considerations**

### **8.1 Access, Rectification, Erasure, or Blockage**

- A Data Subject has the right to obtain from the Data Controller upon request and at reasonable intervals without excessive delay or expense:
  - confirmation in writing as to whether or not Personal Data relating to him/her is being Processed;
  - information as to the purposes of the Processing, the categories of Personal Data concerned, and the Recipients to whom the Personal Data are disclosed;
  - the Personal Data undergoing Processing and of any available information as to its source, communicated in an intelligible form; and
  - the rectification, erasure or blocking of Personal Data when the Processing does not comply with the provisions of the Law, as appropriate.

### **8.2 Objections**

- A Data Subject has the right:
  - to object at any time on reasonable grounds relating to his particular situation to the Processing of Personal Data relating to him/her; and
  - to be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be offered the right to object to such disclosures or uses.

- Where there is a justified objection, the Processing by the Data Controller shall no longer include that Personal Data.

## **9. Enforcement & Penalties**

- 9.1 If the Commissioner determines that a Data Controller has contravened the DPL, the Commissioner may issue an order requiring the Data Controller to refrain from further processing data or doing any related act.
- 9.2 Failure to comply with the Commissioner's order will result in the Data Controller being liable for fines or imprisonment as dictated by Regulation.
- 9.3 A Data Controller can request review of an order from the Commissioner by written request made within 14 days of receipt.
- 9.4 A Data Subject who reasonably believes that he/she has been adversely affected by a contravention of the DPL in respect of the Processing of his Personal Data and as regards the exercise of his rights under specified articles may lodge a complaint with the Commissioner.

## 1. Applicable Law

The UK is a signatory to the European Union Directive on Data Privacy and a member of the European Economic Area (EEA). The UK's national enabling legislation is the Data Protection Act of 1998. The official text is available here:

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

Effective May 26, 2011, the UK amended the Privacy and Electronic Communications Regulations (EC Directive). The official text of the amendment and links to the original directive are available here:

<http://www.legislation.gov.uk/ukxi/2011/1208/made>

## 2. Data Protection Authority and Registration Requirements

- 2.1 The Data Protection Act is enforced by the Information Commissioner ("Commissioner").
- 2.2 Absent an exception, a data controller who processes personal data must register with the Commissioner. Any change to processing of personal data must be amended. The ICO permits online, telephone, and written registration.<sup>18</sup>

## 3. Protected Personal Data

- 3.1 **Personal data** is defined 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 an indication of the intentions of the data controller or any other person in respect to the individual.
- 3.2 **Sensitive personal data** is defined as personal data consisting of information as to race or ethnic origin; political opinion; religious beliefs or other similar beliefs; information pertaining to membership with a trade union; physical or mental health or condition; sex life; commission or alleged commission of any offense; or any proceedings for any offense committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

## 4. Data Collection and Processing

- 4.1 Data may be collected and processed when any of the following conditions are met:
  - consent of the data subject;

---

<sup>18</sup> <https://ico.org.uk/for-organisations/register/>

- data controller needs to process the data because of a pre-contractual or contractual obligation;
- the processing satisfies the data controller's legal obligation;
- the processing protects the vital interests of the data subject;
- the processing is required legally, 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 processing the data, unless the processing would damage a data subject's rights, freedoms or other legitimate interest.

4.2 Sensitive Personal Data may be collected and processed when any of the following conditions are met:

- explicit consent of the data subject;
- processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, subject to exceptions
- processing is necessary in order to protect vital interests of the data subject or another person, subject to certain conditions;
- the processing is carried out by any body or association in the courts of its legitimate activities, subject to certain conditions;
- the information has been made public as a result of steps deliberately taken by the data subject;
- the processing is necessary for the purpose of, or in connection with, legal proceedings, obtaining legal advice, or the exercise or defense of legal rights;
- processing is necessary for the administration of justice or for the exercise of certain government bodies, subject to certain exceptions;
- the processing is necessary for the purposes of preventing fraud, subject to certain conditions;
- the processing is necessary for medical purposes and is undertaken by certain individuals;
- the processing is of sensitive personal data consisting of information as to racial or ethnic origin, so long as other conditions are met and subject to certain exceptions; or
- the personal data are processed in circumstances specified in an order made by the Secretary of State.

## 5. Data Transfer

- 5.1 Data cannot be processed by a third party unless the third party processor provides sufficient guarantees regarding technical and organizational security; the data controller takes reasonable steps to ensure compliance with the Act; and the processing is carried out under a written contract under which the data processor is to act only on instructions from the controller and which requires the processor to comply with obligations equivalent to those imposed on a data controller under the seventh principle under the Act.
- 5.2 International Data Transfer. For any transfer of personal data outside of the EEA, the transfer is allowed without additional requirements so long as the country to which the transfer is being made provides “adequate protection” for the security of the data, or where an exception applies to the adequate exception requirement. Countries with an adequate level of protection include those that have been recognized by the European Commission in accordance with the 1995 European Data Directive 95/46/EC. In addition, transfers to the United States may be permitted pursuant to and in accordance with the US-EU Safe Harbor Framework, or subject to binding corporate rules.<sup>19</sup>

## 6. Data Security

While the UK data protection law does not specify the type of security measures to adopt and implement for the safeguarding of personal data, appropriate technical and organizational measures must be taken to protect against the unauthorized or unlawful processing, accidental loss or destruction or, or damage to, personal data.

## 7. Breach Notification

At the time of publication, there was no mandatory requirement to report data security breach incidents under the Data Protection Act of 1998. The ICO does recommend, however, that if a large number of individuals are affected by a breach incident, the ICO should be informed.<sup>20</sup>

The Privacy and Electronic Communications Regulations requires internet service providers to notify the Commissioner without undue delay, and in some cases, any subscribers, in the event of a breach incident. Failure to notify could result in a fine of GBP 1,000.

## 8. Other Considerations

- 8.1 The Data Protection Act provides individuals a right of access to their personal information. The individual has the right for the data controller to tell him/her about the personal information it holds about him/her, the purposes for which it is being processed, and the recipients or classes of recipients to whom they are or may be disclosed. The individual also has the right to have communicated to him/her in an intelligible form the personal data at issue and any information available to the controller as to the source of the data. In most cases, a response to a valid subject access request is required within 40 calendar days of receipt.

---

<sup>19</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/>

<sup>20</sup> [https://ico.org.uk/media/for-organisations/documents/1562/guidance\\_on\\_data\\_security\\_breach\\_management.pdf](https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf)

- 8.2 At the time of publication there was no requirement that organizations appoint a data protection officer to ensure compliance with the Data Protection Act.

## **9. Enforcement & Penalties**

The Commissioner has full enforcement authority of the UK's data protection law. If the Commissioner learns of a breach of the UK data protection law, the Commissioner can serve an enforcement notice to a data controller to rectify the breach. The Commissioner can impose fines of up to GBP 500,000 for serious violations of the UK's data protection law, where the violation likely to cause substantial damage or distress.

## 1. Applicable Law

Data privacy in Uruguay is governed by the Protection of Personal Data and “Habeas Data” Action 18.331 (“PDHDA”), passed in 2008. *Ley N° 18.331 Protección de Datos Personales y Acción de Habeas Data*. The official text of the Act is available in Spanish here:

<http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor=>. Uruguay’s data protection authority has passed several directives implementing the PDHDA, the most comprehensive of which is *Discreto 414/009*. The official text is available in Spanish here: <http://www.redipd.org/documentacion/legislacion/common/legislacion/uruguay/decreto-414-009.pdf>

## 2. Data Protection Authority and Registration Requirements

### 2.1 Authority. **Unidad Reguladora y de Control de Datos Personales** (Unit for the Regulation and Control of Personal Data (“URCDP”).

The processing of personal data is subject to the PDHDA when it is performed by a database or processing controller whose activities are carried out in Uruguay or where the processing of data is carried out by means of media located within Uruguay.

Exceptions:

- date held by individuals for personal or household use;
- date used for public safety, defense, State security, and law enforcement; or
- date “created and regulated by special laws.”

### 2.2 **Registration.** All databases subject to the PDHDA are required to be registered with the URCDP.

## 3. Protected Personal Data

### 3.1 **Personal data** is defined as any information relating to a person who is identified or identifiable.

### 3.2 **Sensitive data** is defined as personal data revealing racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership or information concerning health or sex life.

## 4. Data Collection and Processing

### 4.1 The data subject of personal data must give prior, informed consent before any collection or processing occurs, except where:

- the data is composed of public information;
- the data is collected during the course of a government function;
- the data collection arises out of a contractual relationship;



- the data is composed of listings limited to the names, surname, identity, nationality, address, and date of birth of the subject, or, in the case of an entity, the business name, assumed name, taxpayer registration, address, telephone number, and owners/officers; or
  - the data is collected exclusively for personal or household use.
- 4.2 Generally, no person may be required to provide sensitive data and it can only be processed with the express written consent of the subject, except:
- sensitive data can be collected and processed if authorized by law to accomplish a compelling public interest; or
  - sensitive data can be collected for statistical or scientific purposes if it is anonymous.

## 5. Data Transfer

### 5.1 International Data Transfer

Generally, the transfer of data to any countries that do not provide appropriate levels of protection as determined by international law is prohibited. The following exceptions to this prohibition apply:

- the transfer is allowed under an international treaty or convention;
  - the transfer is necessary for the exchange of medical data in certain circumstances;
  - the transfer is related to certain bank transfers or exchanges;
  - the transfer is related to international cooperation for the prevention of organized crime, terrorism and drug trafficking;
  - the subject of the data has given unequivocal consent to the transfer;
  - the transfer is necessary for the performance of a contract between the subject of the data and the holder;
  - the transfer is necessary for contractual reasons;
  - the transfer is necessary or legally required on public interest grounds or the establishment, exercise, or defense of right in a judicial proceeding;
  - the transfer is necessary to safeguard the interests of the subject; or
  - the transfer is made from a registry, which according to law or regulation, is intended to provide information to the public or be open to public inspection, subject to certain conditions.
- 5.2 On April 12, 2013, Uruguay acceded to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) and its Additional Protocol. Uruguay was the first non-European country to accede to the convention, perhaps signaling the growing influence of the European Union on data privacy issues. This event comes on the heels of the European Commission's declaration last year that Uruguay's data protection regime was adequate under the European Data Protection Directive. Data privacy in Uruguay is governed by the Protection of Personal Data and "Habeas Data" Action 18.331 ("PDHDA"), which was passed in 2008.

## **6. Data Security**

- 6.1 While the data protection law does not specify the type of security measures to adopt and implement for the safeguarding of personal data, appropriate technical and organizational measures must be taken.

## **7. Breach Notification**

- 7.1 An injured party must be notified whenever anyone in charge of a database learns of a security breach that has the potential of affecting the rights of the injured parties in a significant way.

## **8. Other Considerations**

- 8.1 Right of Habeas Data – Habeas data is a right incorporated into Uruguay’s data protection law that allows an individual to have access to any data about them contained in a database. The law provides a comprehensive process to vindicate this right, but in summary, every person has the right to take legal action to obtain the data about them found in public or private databases. They may also request that the data be removed, updated, or rectified if it can be proven to be incorrect or confidential.
- 8.2 Principal of Finality – The law restricts the use of data for a different purpose than that which they were originally obtained. Additionally, data should be removed when they are no longer necessary or relevant to the purposes for which they were originally collected.

## **9. Enforcement & Penalties**

- 9.1 The URCDP has the authority to sanction database holders for violations of *Ley N° 18.331 Protección de Datos Personales y Acción de Habeas Data*. The sanctions include a warning, fine, and suspension of the database.<sup>21</sup>

---

<sup>21</sup> <http://www.latinlawyer.com/reference/topics/52/jurisdictions/95/uruguay/>