March 2013

DATA PROTECTION LAWS OF THE WORLD

DLA PIPER

ABSTRACT

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

A well-constructed and comprehensive compliance program can solve these competing interests and so represents an effective risk-management tool.

This handbook sets out an overview of the applicable privacy and data protection laws and regulations across 63 different jurisdictions to start you on your way through this complex area of compliance.

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

DLA PIPER'S DATA PROTECTION AND PRIVACY GROUP KEY CONTACTS

EUROPE, MIDDLE EAST AND AFRICA

Cameron Craig
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +44 (0)20 7796 6574
M +44 (0)7971 142 352
cameron.craig@dlapiper.com

Thomas Jansen
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +49 89 2323 72 110
M +49 172 212 8118
F +49 89 2323 72 100
thomas.jansen@dlapiper.com

Patrick Van Eecke
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +32 2 500 1630
M +32 475 680 676
F +32 2 500 6536
patrick.vaneecke@dlapiper.com

Carol Umhoefer
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +33 1 40 15 24 34
M +33 6 61 78 36 88
carol.umhoefer@dlapiper.com

Richard van Shaik
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +31 20 541 9828
M +31 6 5200 5925
richard.vanschaik@dlapiper.com

US, CANADA AND SOUTH AMERICA

Jim Halpert
Partner & Chair of US Data Protection and Data Privacy Group
T +1 202 799 4441
M +1 202 276 5476
F +1 202 799 5441
jim.halpert@dlapiper.com

ASIA-PAC

Alec Christie
Partner & Co-Chair of Asia-Pac Data Protection and Data Privacy Group
T +61292868237
alec.christie@dlapiper.com

INTRODUCTION

Welcome to the second edition of DLA Piper's Data Protection Laws of the World.

We received such a positive response to our first edition that we have updated it and added sections on electronic marketing and online privacy. We have also included entries on Costa Rica, Honduras, Morocco, Panama and Trinidad & Tobago to bring the total number of jurisdictions to 63.

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

These changes are being driven largely by cultural and trade considerations, and by a struggle to keep pace with emerging technology and online business methods. The proposal for a new EU data protection regulation, which is wending its way through the European Parliament as of this writing, is likely to effect a fundamental change in approach to the existing EU framework. However, of equal significance is the toughening of requirements in countries such as Korea, Hong Kong and Singapore, and the emergence of laws in countries which previously had no data protection law in place, including a large number of countries in Asia, Latin America, and the Middle East.

This second edition of the handbook offers a high-level snapshot of selected features of national laws as they currently stand in 63 jurisdictions across the world. It is intended to provide a quick overview of features of data protection law that are often of greatest practical significance to businesses, such as international data transfer restrictions, security obligations and breach notification requirements. It also includes a section on enforcement; an important consideration in assessing the risk presented by any jurisdiction.

The handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements.

Furthermore, enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

DLA Piper's global data protection and privacy team has the deep experience and international reach to help global businesses develop and implement achievable compliance solutions to the myriad data protection laws that apply to global businesses. We have drawn upon our experience of advising on many large data protection projects to develop a standard methodology and proven tools to help businesses achieve a cost-effective robust compliance structure. Should you require further guidance, please do not hesitate to contact us.

EDITORS' FOREWORD

We would like to thank all of the contributors for their invaluable input to this work. We aim to continue to issue annual updates to address major developments in the international data protection landscape.

Inevitably such a work will be out of date almost as soon as it is published, but we shall issue further updates to address major developments in the international data protection landscape via our client alerts and client webinars.

We value your input and feedback. If you have any comments, queries or suggestions in respect of this handbook, please contact any of the editorial team who would very much welcome your comments.

EUROPE, MIDDLE EAST AND AFRICA

Paul McCormack
Solicitor
T +44 20 7796 6140
M +44 796 855 8852
paul.mccormack@dlapiper.com

Cameron Craig
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +44 (0)20 7796 6574
T +44 (0)114 283 3050
M +44 (0)7971 142 352
cameron.craig@dlapiper.com

ASIA-PAC

Arthur Cheuk
Associate
T +852 2103 0501
arthur.cheuk@dlapiper.com

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Data Privacy Group
T +852 2103 0519
M +44 (0)7771 505054
scott.thiel@dlapiper.com

US, CANADA AND SOUTH AMERICA

Kate Lucente
Associate
T +1 813 222 5927
M +1 813 579 7224
kate.lucente@dlapiper.com

Jim Halpert
Partner & Chair of US Data Protection and Data Privacy Group
T +1 202 799 4441
M +1 202 276 5476
jim.halpert@dlapiper.com

CONTENTS

1 Argentina 06
2 Australia 11
3 Austria 17
4 Belgium 22
5 Brazil 28
6 Bulgaria 32
7 Canada 38
8 Chile 45
9 China 50
10 Colombia 54
11 Costa Rica 59
12 Cyprus 62
13 Czech Republic 68
14 Denmark 74
15 DIFC 79
16 Egypt 83
17 Finland 86
18 France 92
19 Germany 99
20 Gibraltar 105
21 Greece 110
22 Honduras 118
23 Hong Kong 121
24 Hungary 125
25 India 131
26 Indonesia 136
27 Ireland 141
28 Italy 148
29 Japan 158
30 Lithuania 164
31 Luxembourg 173
32 Malaysia 183
33 Malta 187
34 Mauritius 195
35 Mexico 203
36 Monaco 210
37 Morocco 215
38 Netherlands 220
39 New Zealand 226
40 Norway 232
41 Pakistan 237
42 Panama 239
43 Philippines 243
44 Poland 251
45 Portugal 260
46 Romania 266
47 Russia 273
48 Singapore 279
49 Slovak Republic 283
50 South Africa 290
51 South Korea 297
52 Spain 307
53 Sweden 312
54 Switzerland 317
55 Taiwan 323
56 Thailand 326
57 Trinidad and Tobago 330
58 Turkey 335
59 UAE 340
60 UK 345
61 Ukraine 351
62 United States 357
63 Uruguay 362

This handbook is provided to you as a courtesy, and it does not establish a client relationship between **DLA Piper** and you, or any other person or entity that receives it. It provides a general overview of the data protection regime currently in force in 63 jurisdictions. It is a general reference document and should not be relied upon as legal advice. The application and effect of any law or regulation upon a particular situation can vary depending upon the specific facts and circumstances, and so you should consult with a lawyer regarding the impact of any of these regimes in any particular instance.

DLA Piper and the other contributing law firms accept no liability for errors or omissions appearing in the handbook and, in addition, **DLA Piper** accepts no liability at all for the content provided by the other contributing law firms. Please note that privacy and information law is dynamic, and the legal regime in the countries surveyed could change.

No part of this publication may be reproduced or transmitted in any form without the prior consent of the **DLA Piper**.

© 2013 DLA Piper UK LLP

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

1. ARGENTINA

CONTRIBUTION DETAILS

cfgd| Cordova Francos Gorbea D'Aiello Jofré ABOGADOS
Marcelo T. de Alvear 814
Buenos Aires – Argentina (C1058AAL)
T +54 11 4311 3571
www.cfgd.com.ar

Sebastian Cordova-Moyano
Felipe Oviedo Roscoe

LAW

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

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

DEFINITION OF PERSONAL DATA

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

DEFINITION OF SENSITIVE PERSONAL DATA

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Argentine Personal Data Protection Agency – in Spanish *Dirección Nacional de Protección de Datos Personales* ("**DNPDP**").
Sarmiento 1118 – 5th Floor
Autonomous City of Buenos Aires
(C1041AAX) Argentina
T +54 11 4383 8512
Website: http://www.jus.gov.ar/datos-personales.aspx

The authority has enforcement power.

REGISTRATION

Any public or private database formed for the purpose of providing reports, any private database which is not formed exclusively for personal use, and any database formed for the purpose of transferring personal data must be registered with the DNPDP. The registration must include, at least, the following information:

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

DATA PROTECTION OFFICERS

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

In general, data controllers may only collect and process personal data with the data subject's consent. Consent is not required if: (i) the data is collected from a publicly accessible database, in the exercise of government duties, or as a result of a legal obligation, (ii) the database is limited to certain basic information, such as name, ID, tax ID, job, birthdate and address, (iii) the personal data derives from a scientific or professional contractual relationship and is used only in such context, or (iv) the information is provided by financial institutions, provided that they were required to do so by a court, the Central Bank or a tax authority.

When collecting personal data, the data collector shall expressly and clearly inform data subjects of: (i) the purpose for which the data is being collected, (ii) who may receive the data, (iii) the existence of a database, the identity of the data collector and its mailing address; (iv) the consequences of providing the data, of refusing to do so or of providing inaccurate information; and (v) the data subject's access, rectification and suppression rights.

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

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

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

TRANSFER

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

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

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

SECURITY

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

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

BREACH NOTIFICATION

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

ENFORCEMENT

The DNPDP is responsible for the enforcement of the data protection regime. Either acting ex officio or upon a complaint from a data subject, the National Ombudsman or consumer associations, the DNPDP is entitled to start an investigation when it suspects that the PDPL has been infringed. Administrative sanctions include warnings, suspension of the right to maintain a database, the imposition of monetary fines, ranging from AR$1,000 to AR$100,000 (approximately US$200 to US$20,000), or the cancellation of the database. In addition, data subjects may separately recover damages for violations of their data protection rights. The PDPL also modified the Argentine Criminal Code to include personal data crimes, such as knowingly inserting false information in a database, knowingly providing false information from a database, illegally accessing a restricted database, or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

revealing information contained in a database that the offender was in charge of keeping confidential. Criminal violations are subject to prison terms ranging from one month up to three years, which may be increased by a 50% if any person suffers damage as a result of the crime

ELECTRONIC MARKETING

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

In particular, the DNPDP's Disposition No. 4/2009 sets forth that (i) all promotional messages shall include the language from the PDPL's Section 27:3 and the third paragraph of Section 27 of Decree No. 1558/01 – which set forth a data subject's right to request suppression of their personal information from marketing databases; (ii) all marketing emails not previously requested or consented to by the data subject shall include as their subject the single word "Publicidad" (promotional); and (iii) senders of promotional messages shall ensure that all mechanisms needed to honour the data subject's requests are in place.

ELECTRONIC PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

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

Particularly with regard to automatic data collection programs, the current interpretation of most scholars is that information collected by "cookies" or similar programs does not qualify as "personal data" because such information corresponds to a device and not to the user him or herself.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

2. AUSTRALIA

CONTRIBUTION DETAILS

Alec Christie
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com

Reyhaneh Saadati
Solicitor
T +61 2 9286 8509
reyhaneh.saadati@dlapiper.com

LAW

Data protection in Australia is currently a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Cth) and its National Privacy Principles applies to private sector businesses and its Information Privacy Principles apply to all Commonwealth Government and Australian Capital Territory Government agencies ("**Privacy Act**").

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

- Information Act 2002 (Northern Territory);
- Privacy and Personal Information Protection Act 1998 (New South Wales);
- Information Privacy Act 2009 (Queensland);
- Personal Information and Protection Act 2004 (Tasmania); and
- Information Privacy Act 2000 (Victoria).

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

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 **("New Act")** was passed by the Australian parliament in December 2012 and comes into force from March 2014. The New Act contains significant reforms to the Privacy Act, including replacing the National Privacy Principles for the private sector and Information Privacy Principles for Commonwealth and Australian Capital Territory Government agencies with a single consolidated set of principles

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

referred to as the Australian Privacy Principles ("**APPs**"). The New Act also significantly strengthens the powers of the Australian Information Commissioner to conduct investigations and ensure compliance with the amended Privacy Act.

Given the New Act does not come into force until March 2014, here we outline the obligations currently imposed under the Privacy Act and highlight only those key new obligations which will come into force from March 2014.

DEFINITION OF PERSONAL DATA

Personal Data (which is referred to as 'personal information' in Australia) 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.

DEFINITION OF SENSITIVE PERSONAL DATA

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

Information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- record;

that is also personal information; or

- health information about an individual; or
- genetic information about an individual that is not otherwise health information.

The New Act expands the definition of 'sensitive information' to also include:

- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; and
- biometric templates.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Australian Information Commissioner is the national data protection regulator responsible for overseeing the Privacy Act.

REGISTRATION

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

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer, but it is good and usual practice.

COLLECTION AND PROCESSING

An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. The New Act further limits collection of personal information by requiring it to be "reasonably necessary" for one or more of the organisation's functions or activities.

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

- its identity and how to contact it;
- why it is collecting (or how it will use the) information about them;
- to whom it might give the personal information;
- the fact that the individual can obtain access to their personal information;
- any law requiring the collection of personal information; and
- the main consequences (if any) for the individual if all or part of the information is not provided.

Under the New Act the organisation must also take reasonable steps to make an individual aware of:

- the fact that the organisation's privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organisation will deal with such complaint; and
- whether the organisation is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Organisations usually comply with this requirement by including the above information in a privacy policy and requiring individuals to accept that privacy policy prior to giving their personal information.

An organisation must not use or disclose personal information about an individual unless:

- it is for the primary purpose of collection or a secondary purpose related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for that secondary purpose;
- the individual consents;
- the information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual's consent and (among other things) the individual is told that they can opt out of receiving marketing from the organisation;
- it is for research or statistics relevant to public health or safety;
- there is a serious threat to health and safety and using or disclosing personal information will help reduce that threat; or
- it is required or authorised by law or on behalf of an enforcement agency.

Under the New Act, in the case of use and disclosure for the purpose of direct marketing, organisations are required to also ensure that:

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

Where "sensitive information" is processed there are additional protections under the Privacy Act which generally provide that an organisation is not allowed to collect sensitive information from an individual unless certain limited requirements are met, including that:

- the individual has consented (under the New Act, as well as having the consent of the individual the sensitive information must be reasonably necessary for one or more of the entity's functions or activities);
- collection is required or authorised by law;
- the information is required to establish or defend a legal or equitable claim; or
- the individual is incapable of consenting and the information is needed because of a serious and imminent threat to the life or health of the individual.

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

Personal information may only be transferred outside of Australia or to a different organisation (including a parent company) where:

- the organisation reasonably believes that the information is subject to a law, binding scheme or contract which effectively provides for no less protection than the Privacy Act (under the New Act there can be no reliance on contractual provisions and the organisation must also ensure that there are mechanisms that the individual can access to take action to enforce the protections of that law or binding scheme);
- the individual consents to the transfer (under the New Act the organisation must, prior to receiving consent, expressly inform the individual that if he or she consents to the disclosure of the information the organisation will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs);
- the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre contractual measures taken in response to the individual's request (under the New Act personal information will no longer be able to be transferred outside of Australia relying on this);
- where the transfer is for the benefit of the individual, it is impractical to obtain their consent and if it were practical, they would be likely to give their consent (under the New Act personal information will no longer be able to be transferred outside of Australia relying on this); or
- where the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed inconsistently with the Privacy Act (under the New Act, where the organisation transfers data to an overseas recipient on this basis, the organisation will remain liable for any breach of the APPs by the overseas recipient).

SECURITY

Any personal information that an organisation retains must have appropriate security measures in place to protect that information from misuse and loss and from unauthorised access, modification or disclosure. An organisation must also take reasonable steps to destroy or permanently de identify personal information if it is no longer needed.

BREACH NOTIFICATION

An organisation that breaches the Privacy Act is currently under no legal obligation (and it is not generally current practice) to report that breach to the affected individual(s) or the Australian Information Commissioner.

ENFORCEMENT

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Under the New Act the Australian Information Commissioner will also be able to investigate breaches of the new APP 1 regarding "open and transparent management of personal information" on its own initiative (i.e. where no complaint has been made).

After investigating a complaint, the Australian Information Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organisation rectify its conduct or that the organisation redress any loss or damage suffered by the complainant. Under the New Act fines of up to A$220,000 for an individual and A$1.1 million for organisations may be requested by the Australian Information Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals.

ELECTRONIC MARKETING

The sending of electronic marketing (which is referred to as 'commercial electronic messages' in Australia) is regulated by the *SPAM Act* 2003 (Cth) ("**SPAM Act**").

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

A failure to comply with the SPAM Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to A$1.1 million per day.

E-PRIVACY AND COOKIE COMPLIANCE

There are no laws or regulations in Australia, beyond the application of the Privacy Act and State and Territory privacy laws specific to e-privacy, the collection of location and traffic data, or the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organisation must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

3. AUSTRIA

CONTRIBUTION DETAILS

Wolfgang Freund
Partner
T +43 1 531 78 1401
wolfgang.freund@dlapiper.com

LAW

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

DEFINITION OF PERSONAL DATA

Personal Data is defined as information relating to an identified or identifiable subject.

DEFINITION OF SENSITIVE PERSONAL DATA

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

NATIONAL DATA PROTECTION AUTHORITY

Austrian Data Protection Commission

Datenschutzkommision

REGISTRATION

- Unless an exemption applies, data controllers who process personal data by automatic means must notify the Data Protection Authority **("DPA")**, who keep a register of all data applications. The Data Protection Register is accessible by the public. Changes to the data application will require the notification to be amended.
- An exemption applies to so called standard applications, which are defined by decree of the Federal Chancellor.
- The notification shall inter alia include the following information (as outlined in the DPA standard notification form):
- the title and purpose(s) of the data application;
- the controller's contact details and if relevant the controller's representatives' contact details;
- the categories of personal data processed;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

DATA PROTECTION OFFICERS

There is no legal requirement in Austria for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

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

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies. The notification shall at least include information on the identity of the controller and the purposes of the processing. The data controller should also inform the data subject of other aspects necessary to ensure that the processing is fair, such as whether or not it is obligatory to respond and the right to object to the processing.

TRANSFER

A transfer of personal data is only lawful, if:

- the data originates from a lawful data application;
- the recipient can show a legitimate authority to receive the data; and
- the interests of the data subjects are preserved.

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

- the recipient resides in a country, which by decree of the Federal Chancellor provides for "adequate protection" (e.g. companies which adhere to the US/EU Safe Harbor principles);
- the data subject has without any doubt consented to the transfer;
- a contract between the controller and the data subject or a third party, that has been concluded clearly in the interest of the data subject, cannot be fulfilled except by the trans-border transmission of data;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

The DPA shall grant its approval if, in the specific case, adequate protection can be evidenced. Such safeguards may inter alia result from contractual clauses, e.g. by standard contractual clauses approved by the European Commission, or via an organisation's Binding Corporate Rules.

SECURITY

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

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

BREACH NOTIFICATION

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

ENFORCEMENT

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

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

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

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Online privacy is specifically regulated by the TKG.

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

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

4. BELGIUM

CONTRIBUTION DETAILS

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

LAW

Belgium implemented the EU Data Protection Directive 95/46/EC with the Data Protection Act dated 8 December 1992 ("**Act**"). Enforcement is ensured by the Data Protection Authority ("**DPA**").

DEFINITION OF PERSONAL DATA

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

A person is considered to be an identifiable person when he or she can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

DEFINITION OF SENSITIVE PERSONAL DATA

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

- personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life or trade union membership;
- health related data personal data; and
- personal data relating to disputes which have been submitted to courts and tribunals as well as to administrative judicial bodies, regarding suspicions, prosecutions or convictions in matters of crime, administrative sanctions or security measures.

NATIONAL DATA PROTECTION AUTHORITY

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

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

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

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

DATA PROTECTION OFFICERS

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

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

As part of this obligation the DPA has issued "Security Guidelines", which reflect what is to be considered as constituting 'adequate technical and organisation security measures'. Although the Security Guidelines are not part of the Act itself and are not binding, they do have an important moral value.

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

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

- the data subject consents;
- the processing is necessary to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract;
- the processing is necessary to enable the controller to fulfil a legal obligation;
- the processing is necessary to protect the vital interests of the data subject;
- the processing is necessary to perform a task in the public interest;
- the processing is necessary to exercise official authority; or
- the processing is necessary to enable the controller or third parties to whom the data is disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject.

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

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

TRANSFER

Transfer of a data subject's personal data to non EU/European Economic Area countries is allowed if the countries provide "adequate protection".

For the transfer of data to the United States, companies which adhere to the US/EU Safe Harbor principles are deemed to offer adequate protection.

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

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

Currently, in the context of a notification procedure, the DPA usually requests a copy of data transfer agreements, in particular to verify whether any changes were made to the EU model clauses. No formal approval of EU model clauses based data transfer agreements is required.

However, the DPA recently indicated that in the near future, this could change and an authorisation decree may be required for each contract based international transfer of personal data – regardless of whether the international transfer is based on the EU Model Clauses.

SECURITY

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

The DPA has issued (non binding) guidelines in respect of such security measures.

BREACH NOTIFICATION

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

ENFORCEMENT

The DPA is authorised to investigate complaints, and to act as a mediator in case of complaints. The DPA may also appoint experts, may require the provision of documents, and may require access to certain places. In the case of criminal actions, the DPA must notify the public prosecutor.

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

ELECTRONIC MARKETING

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Additionally, specific rules are set out in Belgian E-Commerce Act (Act of 11 March 2003) regarding opt-in requirements:

- These rules apply to all "electronic messages", i.e. traditional emails, text messages (Short Message Systems or SMS), etc. Other types such as instant messaging and chat may also fall within the scope of these rules depending on the specific context. This covers not only clear promotional messages, but also newsletters and similar communications. Indeed, 'any form of communication intended for the direct or indirect promotion of goods, services, the image of a company, organization or person which/who exercises a commercial, industrial or workmanship activity or regulated profession' falls within the scope of these rules.
- As a general principle, the prior, free, specific and informed consent of the recipient of the message must been obtained ('opt-in principle').
- Two exceptions apply to the opt-in principle. No prior, free, specific and informed consent is to be obtained if:
  - the electronic marketing message is sent to existing customers of the service provider; or
  - the electronic message is sent to legal persons (e.g. to a general email address such as info@company.com).
- These exceptions are, however, subject to compliance with strict conditions. The exception applicable to existing customers for instance requires that the electronic marketing message sent to such existing customer relates to goods or services similar to those goods or services purchased by the customer.
- All electronic messages must contain a clear reference to the recipient's right to opt out, including means to exercise this right electronically.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookies

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

The use and storage of cookies and similar technologies requires: a) clear and comprehensive information; and b) consent of the website user.

Consent is not required for cookies that are:

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

Regulatory guidance on the informed consent requirement is expected to be issued in the near future.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Location data

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

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

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

Traffic data

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

5. BRAZIL

CONTRIBUTION DETAILS

Murta Goyanes Advogados
Avenida Rio Branco, 1, 1709
Centro, Rio de Janeiro, RJ CEP: 20090-003
T +55 21 3553 6575
www.murtagoyanes.com.br

Marcelo Goyanes
Founding Partner
M +55 21 8208 6103
marcelo.goyanes@murtagoyanes.com.br

Luis Henrique Porangaba
Founding Partner
luis.porangaba@murtagoyanes.com.br

LAW

Brazil does not have a law that is specifically devoted to data protection. However, there are general principles and provisions on data protection and privacy in the Federal Constitution, in the Brazilian Civil Code and in laws and regulations that address particular types of relationships (eg the Consumer Protection Code[1] and labor laws), particular sectors (eg financial institutions, health industry, telecommunications etc.), and particular professional activities (eg medicine and law). Additionally, there are laws on the treatment and safeguarding of documents and information handled by governmental entities and bodies that have privacy implications.

The Federal Constitution provides that (i) the intimacy, private life, honour and image of persons are inviolable; (ii) the confidentiality of correspondence and electronic communication is protected; and (iii) everyone is ensured access to information, although the confidentiality of the source shall be safeguarded whenever necessary for the exercise of a professional activity.

Discussion of privacy legislation has increased recently. The National Congress is reviewing several bills that address data protection, and the Executive Branch presented a new proposal for a specific data protection and other internet related issues law on August 24, 2011, which has been presented to Congress for consideration.

On November 30, 2012, the National Congress enacted computer crime Law 12,737/2012, which criminalizes the acts of hacking or invading electronic devices with intent to obtain, adulterate or destroy data and/or information without the consent of the owner of the device.

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF PERSONAL DATA

There is no legal definition of "personal data" established in a particular statute. In general, it should be considered to include any particular information related to an individual, including name, age, sex, profession, address, religion, sexual orientation, criminal background, as well as any personal communication exchanged without any intent to go public, such as personal emails and messaging.

DEFINITION OF SENSITIVE PERSONAL DATA

There is no legal definition of "sensitive data" or the equivalent.

NATIONAL DATA PROTECTION AUTHORITY

Brazil does not have a national data protection authority.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer.

COLLECTION AND PROCESSING

In general, there is no requirement to obtain prior consent to collect personal data submitted by the subject. However, the use, treatment and protection of such data are subject to some restrictions. Some specific statutes and case law establish that the scope of collection, treatment and use of personal data must be restricted to the purpose for which the data was originally collected. There is also a common understanding that certain sensitive data (eg religion, sexual orientation, criminal background etc.) should not be collected and used for any discriminatory purpose; if a company collects and uses such sensitive data it should obtain the person's consent.

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

TRANSFER

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

In view of applicable general principles, data processors in Brazil are required to take reasonable technical, physical and organizational measures to protect the security of personal data, but, generally, there are no specific requirements, restrictions or details on how security should be implemented. Case law establishes that service providers and networks should keep access records (such as IP addresses, logins etc) so as to identify users who may have committed crimes, defamation or acts of infringement. If such records are not kept for a reasonable period of time, the service provider or network may be held jointly liable for an act of infringement.

BREACH NOTIFICATION

Security breach notification is not required.

Nevertheless, in view of the recently enacted hacking Law 12,737/2012, the owner of the personal data or the breached device may – although not obligated to do so – notify public authorities in order to conduct enquiries, so as to identify and prosecute the individual responsible for the crime of hacking and/or invasion of protected device established therein.

ENFORCEMENT

Currently, there is no data protection authority. Enforcement can occur through administrative procedures, individual civil suits or class actions, which can be initiated by the data subject, by public authorities (eg State Attorney's Office, Consumer Protection Office and the regulator for the relevant industry) or by associations that defend collective interests.

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

Administrative fines related to consumer issues can be established in amounts up to R$3 million (approx. US$1.5 million). Damage awards may vary but in actions brought by a single consumer should not surpass R$15,000 (approx. US$7,500), while class actions may reach values far above US$1 million.

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

There is no federal law specifically addressing electronic marketing.

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

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

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

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no law specifically addressing online privacy.

Nevertheless, the established rights of privacy, intimacy and consumer rights apply equally to electronic media, such as mobile devices and the Internet.

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

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

6. BULGARIA

CONTRIBUTION DETAILS

Wolf Theiss
Rainbow Centre, 29 Atanas Dukov Street
1407 Sofia, Bulgtaria
www.wolftheiss.com

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

LAW

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

The Act was last amended by the State Gazette, Issue No. 81 of 29 December 2011.

DEFINITION OF PERSONAL DATA

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

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data means personal data:

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The Bulgarian data protection authority ("**DPA**") is the Personal Data Protection Commission (*In Bulgarian: Комисия за защита на личните данни*):
15 Akademik Ivan Evstatiev Geshov Str.
Sofia 1431
Bulgaria
kzld@cpdp.bg
www.cpdp.bg

REGISTRATION

Unless an exemption applies, prior to initiating any personal data processing data controllers must apply for registration with the DPA. The registration covers the data controller and the personal data registers controlled by it. Changes to the initial registration will require notification of the DPA prior to implementing such changes. The registration is free of charge. The DPA support the following public registers:

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

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

- Application Form covering data controllers' details, such as:
  - the controller's identification details;
  - the controller's location;
  - whether the controller processes data for the purposes of defence, national security, public order or criminal proceedings;
  - the controller's main activity;
  - whether the purpose and the means of processing are determined by the controller or by the law;
  - whether the data is processed by the controller or data processor; or
  - the number of data registers.
- Registry Description Form covering each separate register:
  - name and full address of the register;
  - the purpose(s) of the processing;
  - legal ground of the processing;
  - whether automatic or non automatic means are used;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the categories of data subjects;
- the categories of personal data processed, including sensitive data (if processed);
- the recipients or categories of recipients of the personal data;
- whether a data transfer to foreign countries is required and the specific countries;
- sources for collection of the data;
- whether an explicit consent of the data subjects is available; and
- descriptions of technical and organisational measures for data protection in accordance with DPA regulation.

Exemptions apply in the following situations:

- data controllers operating the public register on the basis of law which is publicly accessible or accessible to those who have a legal interest;
- non profit making organisations carrying out enumerated processing; and
- data controllers explicitly exempt from registration by the DPA on the basis that the processing does not endanger the rights and legal interests of data subjects. The rules and conditions for this exemption are specified in a special regulation of the DPA. In such cases the data controller should apply for and obtain the DPA's decision on the exemption of registration. However, such decision would not relieve the respective data controllers from the DPA's control under the Act.

DATA PROTECTION OFFICERS

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

At the beginning of 2009 the DPA proposed a Draft Amendment of the Act and initiated public discussion. One of the proposed amendments provided an obligation on data controllers to appoint a specially trained DPO. The Draft Amendment is still under discussion and internal preparation by the DPA, but it is a sign of its understanding of the necessity of a DPO.

COLLECTION AND PROCESSING

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

- processed fairly and lawfully;
- processed only for specific and legal purposes and used only for the purposes stated at the time it is collected;
- adequate, relevant and not excessive for the purposes for which it is processed;
- accurate, complete and where necessary kept up to date;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- not kept in a personally identifiable form longer than necessary;
- processed in accordance with the rights of the data subject under applicable law;
- kept securely; and
- not transferred to countries that do not have adequate data protection laws unless the data exporter takes certain specific steps to ensure that the data is adequately protected.

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

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

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

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

- identification data of the controller and its representative;
- the purposes for which the data will be processed;
- the recipients or categories of recipients to whom the personal data may be disclosed;
- whether the provision of personal data is obligatory or voluntary and the consequences if the data is not provided (applicable if the data is gathered directly from the person to whom it relates);
- the categories of personal data relating to the respective individual (applicable if the data is not gathered directly from the data subject); or
- information about the right of access to the data and the right to rectify the collected data.

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

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

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

The DPA should not undertake an assessment where a decision of the European Commission has to be implemented whereby the European Commission has ruled that (1) the country to which the personal data are transferred has ensured an adequate level of protection; or (2) certain appropriate contractual clauses are in place ensuring the adequate level of protection (the EU model contractual clauses).

The DPA has still not issued any statement of approval or recognition regarding the use of binding corporate rules ("**BCR**"). Should the DPA consider that the protection level of personal data protection in the recipient state is unsatisfactory, it may prohibit the personal data transfer. Even in such a case, the DPA may authorise the transfer should the data controller provide sufficient warranties with respect to the protection of the individual's fundamental rights. In any case, the data controller should notify in advance the DPA of its intention to transfer personal data to countries outside the EU and EEA by specifying the countries of transfer, the purpose of the transfer and the categories of personal data subject to transfer.

SECURITY

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

The minimum level of technical and organisational measures, as well as the admissible type of protection are specified by the DPA in a regulation. The Act requires data protection measures to be specified in an internal instruction issued by the data controller and to be announced in the registration application before the DPA.

BREACH NOTIFICATION

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

ENFORCEMENT

The DPA is responsible for the enforcement of the Act. Either acting ex officio or upon a complaint from a data subject the DPA is entitled to: (i) initiate an investigation; (ii) provide mandatory instructions, including but not limited to order the database to be erased when it does not comply with the data protection regulations; (iii) provide a mandatory term for rectification of the breach; (iv) temporarily prohibit any unlawful data processing, after

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

preliminary notification (temporary prohibition of data processing could be imposed also in case of failure by the data controller to comply with the Commission's mandatory instructions); and (v) impose administrative sanctions.

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

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

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

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

ELECTRONIC MARKETING

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

There are grounds for lawful processing of personal data (as mentioned above) but taking into account their limited and specific scope, for e-marketing specific purposes, the explicit consent of the data subject is likely to be necessary. The absence of a special legal framework concerning exclusively data protection in e-marketing makes the opt-in regime the only possible legitimate method of pursuing e-marketing. This is further supported by the current regulations concerning direct marketing activities.

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

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Again, neither the current Personal Data Protection Act, nor any other legislative act in force, recognises a specific framework or protection for processing of personal data as part of any kind of online activities, including cookies and traffic and location data. In the absence of specific rules, the general regime for processing of personal data shall apply and the data controller shall insure one of the above mentioned grounds to process the data lawfully is satisfied.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

7. CANADA

CONTRIBUTION DETAILS

Heenan Blaikie LLP
Offices: Montreal * Toronto * Vancouver * Quebec * Calgary
Sherbrooke * Ottawa * Trois-Rivieres * Victoria * Paris * Singapore
www.heenanblaikie.com

Adam Kardash
Partner
T +1 416 360 3559
akardash@heenan.ca

LAW

In Canada there are 27 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti spam legislation, identity theft/criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, and remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

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

- Personal Information Protection and Electronic Documents Act ("**PIPEDA**");
- Personal Information Protection Act ("**PIPA Alberta**");
- Personal Information Protection Act ("**PIPA BC**"); and
- An Act Respecting the Protection of Personal Information in the Private Sector ("**Quebec Privacy Act**"), (collectively, "**Canadian Privacy Statutes**").

PIPEDA applies (i) to organisations that are deemed to be a "federal work, undertaking or business" (eg banks, telecommunications companies, airlines, railways, and other interprovincial undertakings); (ii) to organisations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted "substantially similar" legislation (PIPA BC, PIPA Alberta and the Quebec Privacy Act have been deemed "substantially similar"); and (iii) to inter provincial and international collection, use and disclosure of personal information.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF PERSONAL DATA

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

DEFINITION OF SENSITIVE PERSONAL DATA

Not specifically defined.

NATIONAL DATA PROTECTION AUTHORITY

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

REGISTRATION

There is no registration requirement under Canadian Privacy Statutes.

DATA PROTECTION OFFICERS

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

COLLECTION AND PROCESSING

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

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Each of the Canadian Privacy Statutes also provides individuals with (i) a right of access to personal information held by an organisation, subject to limited exceptions, and (ii) a right to correct inaccuracies in/update their personal information records.

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

TRANSFER

When an organisation transfers personal information to a third party service provider (ie who acts on behalf of the transferring organisation), the transferring organisation remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation. In particular, the transferring organisation is responsible for ensuring that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third party service providers in and outside of Canada, in their privacy policies and procedures.

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

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

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

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

SECURITY

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

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

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

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

On 29 September 2011, proposed amendments to PIPEDA were introduced that, if passed, would require that organisations report to the OPC "*any material breach of security safeguards involving personal information under its control*". The proposed amendments also require organisations to notify an affected individual "*if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual*". The proposed amendments are not yet in force.

ENFORCEMENT

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

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

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organisations are required to comply with the order within a prescribed time period, or apply for judicial review. Similarly, under the Quebec Privacy Act, an order must be complied with within a prescribed time period.

PIPA Alberta and PIPA BC also lay out a number of offences, including, but not limited to, obstructing the Commissioner, knowingly making a false statement to the Commissioner, punishing whistleblowers, disposing of information to evade an access request, and failing to comply with an order. In BC, these offences also include the use of deception or coercion to collect personal information. In Alberta, these offences also include the collection, use, or disclosure of personal information contrary to the Act and failure to provide notice of a breach. Offences are punishable by a fine of not more than $10,000 for individuals and $100,000 otherwise.

Under PIPA Alberta and PIPA BC, where an order has been issued against an organisation or an organisation has been convicted of an offence under the legislation, individuals have a cause of action against the organisation for damages for loss or injury suffered as a result of the organisation's breach of its obligations under the legislation.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed above), as well as Canada's Anti-Spam Legislation ("**CASL**"). CASL received Royal Assent on December 15, 2010 and is expected to be in force by early 2014.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

What constitutes both permissible express and implied consent is defined in the Act and regulations. For example, an organization may be able to rely on implied consent when there is an existing business relationship with the recipient of the message, based on (i) a purchase by the recipient within the past two years; or (ii) a contract between the organization and the recipient currently in existence or which expired within the past two years.

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

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

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

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

For example, in the context of social media, the OPC has released numerous Reports of Findings addressing issues including: default privacy settings; social plug-ins; identity authentication practices; and the collection, use and disclosure of personal information on social networking sites. The OPC has also released decisions and guidance on privacy in the context of Mobile Apps.

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

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

- Individuals are made aware of the purposes for the online behavioural advertising, at or before the time of collection, in a manner that is clear and understandable;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Individuals are informed of the various parties involved in the online behavioural advertising at or before the time of collection;
- Individuals are able to opt-out of the practice and the opt-out takes effect immediately and is persistent;
- The information collected is non-sensitive in nature (i.e. not health or financial information); and
- The information is destroyed or made de-identifiable as soon as possible.

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

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

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

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

8. CHILE

CONTRIBUTION DETAILS

Claro y Cía.
Apoquindo 3721
Piso 14
Las Condes, Santiago, Chile
T +56 2 367 3000
www.claro.cl

Eduardo González
Partner
T +56 2 367 3017
egonzalez@claro.cl

Patricio Middleton
Senior Associate
T +56 2 367 3007
pmiddleton@claro.cl

LAW

Chile has enacted the following laws and regulations regarding the protection of personal data:

- Law No. 19,628 concerning the protection of personal data applicable to the public and private databases (last amended by Law No. 20,575 of February 17, 2012);
- Decree No. 779 (year 2000) of the Ministry of Justice, concerning the regulations applicable to databases of personal data maintained by public entities;
- Law No. 20,285 that regulates access to the public information and protects personal data in article 5 (first paragraph), article 21 No. 2 and article 33 m); and
- Decree No. 13 (year 2009) of the General Ministry of the Presidency, containing regulations implementing Law No. 20,285.

DEFINITION OF PERSONAL DATA

Personal data means any information concerning identified or identifiable natural persons.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive data means personal data regarding the physical or moral characteristics of an individual, facts or circumstances of an individual's private life or intimacy, such as personal habits, race, ideologies, political opinions, beliefs or religious convictions, current physical or psychological health status, and sex life.

NATIONAL DATA PROTECTION AUTHORITY

The *Jueces de Letras* (first instance courts), the Appeal Courts and the Supreme Court serve as the national authorities in charge of the protection of the personal data. The *Consejo para la Transparencia* has authority regarding the personal data held by any public entity.

REGISTRATION

Chilean law contains only one registration requirement in respect of databases of personal data held by public entities. This registry is maintained by the Servicio de Registro Civil (article 22, Law No. 19,628).

There is no registration requirement for private databases (although private databases may be registered for IP protection purposes on the national Intellectual Property Registry, according to the Law No. 17,334).

DATA PROTECTION OFFICERS

The distributors of registries or databases that contain personal data of an economic, financial, banking or commercial nature, must appoint a natural person in charge of the treatment of the personal data, with whom the data subjects exercise his/her rights granted under Law No. 19,628 (e.g. the right to request an accounting of information held and disclosed by the database owner during the previous 12 months).

COLLECTION AND PROCESSING

Under Law No. 19,628, the processing or use of personal data is only permissible under the following specific circumstances:

- Where expressly authorised by the Law;
- With the express authorization of the individual data subject;
- When the personal data have been collected from public sources;
- When the personal data is economical, financial or commercial in nature;
- When the information is contained in listings related to a specific category of individuals that only disclose information such as the allegiance of such individual to such specific group, his/her profession or activity, educational diplomas, address and date of birth;
- By a private legal entity for the exclusive use of the entity, its affiliates and associates; and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- By entities affiliated with any of the abovementioned legal entities that use the information for statistical purposes, price listing purposes or other purposes for the general benefit of its associates.

When the personal data concerns economic, financial or commercial obligations, Chilean law imposes special obligations:

- such data may only be processed for the purposes of assessing credit risk or processing credit approvals;
- disclosure of such data can only be made to "established merchants" and entities that participate in the credit risk assessment, and then only for the purposes of credit approval;
- such data cannot be requested during processes of personnel selection, pre-school admission, undergraduate or graduate admissions, emergency medical care or application for a public office;
- controllers of such databases or distributors of such registries or databases, in carrying out their business, must adhere to the following principles: legitimacy, access and opposition, information, quality of data, finality, proportionality, transparency, non-discrimination, limits of use and security in treatment of personal data. In the event of a civil complaint by a data subject, the controller has the burden of proof in demonstrating to the judge that the controller exercised due diligence in its treatment of personal data;
- distributors of registries or databases of such nature shall have a registration system that tracks access and delivery of personal information, identifying the name of the person or entity who requested the information, the purpose, date and time of the request, and the person responsible for the delivery of the information. Data subjects (referred to as data holders under Chilean law) may request, every 4 months and at no cost, an accounting of the information registered in such system during the last 12 months;
- data subjects may request that the entities responsible for such databases provide to them a certificate of the past due credit obligations registered in such databases (which is different from a general credit risk assessment);
- the database controllers may only communicate personal data regarding past due credit obligations where the default of the individual is unquestionable;
- the database controllers may not communicate obligations that have already been extinguished, or whose due dates and conditions have been extended, renegotiated, novated, or that became payable more than 5 years earlier; and
- the law suspends communication regarding any debts of the unemployed (until the person becomes employed).

In any case, personal data must be precise, updated and consistent with the real situation of the individual to whom the data relates. Furthermore, data obtained from non public sources may only be used for the purposes for which they were collected.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The law expressly prohibits any kind of predictive models or commercial risk scorings that are not based solely on objective information concerning delinquencies or rejected/retuned negotiable instruments (e.g. checks) of individuals or entities. An individual affected by a violation of this prohibition may require that the information be immediately eliminated from the database and may seek damages against the responsible entity.

The processing of sensitive data is permitted only: (i) where expressly authorised by the law; (ii) with the consent of the data subject; or (iii) for the purpose of providing health benefits.

The Law No. 19,628 entitles any person to request from a public or private entity information regarding: (i) his/her personal data held by the entity; (ii) the source of the data; (iii) the purpose of storage; and (iv) the identity of the persons or entities that have received his or her personal data from the entity. The data subject's right to request access to, demand modification or deletion of, or to block future use of his or her personal data, cannot be limited by agreement.

TRANSFER

The transfer or disclosure of personal data is subject to substantially the same restrictions as those applicable to collection and processing.

SECURITY

Entities may be liable to data subjects for security breaches. The party responsible for any database of personal data has a duty to protect the information it contains and is responsible for any damages suffered as a result of non compliance with this obligation.

Chilean law regulates the security of any electronic transmission of personal data. The law states that the database owner may use an automatic procedure to transfer personal data, provided that the rights of the individuals are safeguarded and the transmission relates to business purposes of the parties to the communication. Further, for any electronic transmissions, an entity must keep a record of the: a) identity of the person requiring the information; b) motive and purpose of the transfer; and c) kind of data that is transmitted.

Chilean law mandates that any employees of public or private entities who handle personal information are subject to a confidentiality obligation that extends after the termination of their employment agreement. However, it does not require implementing specific security measures.

BREACH NOTIFICATION

In Chile, there is no duty to notify a data subject or regulator when personal data is lost or stolen.

ENFORCEMENT

If the owner controller of a registry or database, does not respond to a data subject's request within 2 business days, or denies the request, the data subject may file a claim before the *Juez de Letras* for the protection of his or her rights. Any decision of the *Juez de Letras* may be appealed to the relevant Appeals Court. The Supreme Court determines cases where access is denied based upon a national security or the national interest.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Courts are authorised to impose a fine of 2 to 50 UTM (as of this writing approximately US$170 to $4,250).

In addition, Law No. 20,285 provides that any person may demand a public entity to eliminate any of his or her data collected, processed or stored in violation of the applicable law. If the public entity denies the request or if it does not provide any answer, the data subject may file a claim before the *Consejo para la Transparencia*. The resolution of the *Consejo para la Transparencia* may, in turn, be appealed before the Appeals Court of Santiago. Violations of personal data laws may also result in disciplinary procedures against a public entity.

It is also a criminal offense to do any of the following:

- Destroy or disable all or part of a system for the treatment/protection of personal information;
- Block or modify the functioning of a database;
- Appropriate, use or unlawfully obtain knowledge of the personal information included in a database or to unlawfully intercept, interfere with or access personal data or databases;
- Alter, damage or destroy the data contained in a database; or
- To reveal or to disclose the data contained in an information system.

ELECTRONIC MARKETING

Article 28B of the Consumer Protection Law provides that any promotional or advertising communication sent by electronic mail shall indicate the subject matter, the identity of the sender and a valid address to which the recipient may opt out of receiving future communication (opt-outs must be honored immediately).

Promotional emails that are anonymous emails or that do not contain all the required information violate the law.

If the company sends any promotional email to a consumer after the consumer's opt-out request, the sender is subject to a fine up to 50 UTM (approximately US$4,250).

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Chile does not have an online privacy law that regulates cookies, location data or other conventional means of online tracking. However, Law No. 19,223 protects online privacy by criminalizing the following conduct, among others:

- To intercept, interfere with or access to an information system with the purpose of taking possession, using or unlawfully obtaining knowledge about the information contained in such system; or
- To maliciously reveal or disclose the data contained in an information system.

The wording of Law 19233 is very broad. It is possible that a court could consider that the use of cookies and other similar tracking devices under certain circumstances is a violation of the law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

9. CHINA

CONTRIBUTION DETAILS

Belinda Tang
Associate
DLA Piper UK LLP Beijing Representative Office
T +86 10 6561 1788 ext. 827
M +86 1352 272 1802
belinda.tang@dlapiper.com

LAW

Provisions relating to personal data protection are found in various laws and regulations, but none of the provisions clearly define the scope of privacy rights. The main provisions are found in the General Principles of Civil Law and the Tort Liability Law, which define such rights as a right of reputation or right of privacy. A draft Personal Data Protection Law has been under review by the government for many years, but there is still no indication as to if and when such law will be passed.

The Ministry of Information and Industry of China ("**MIIT**") has published draft guidelines called the Information Security Technology – Guide for Personal Information Protection ("**Draft Guidelines**").

In 28 December 2012, the decision on strengthening online information protection (the "**Decision**") was adopted by the Standing Committee of the National People's Congress (NPC). The purpose of the Decision is to protect internet information security, safeguard the lawful rights and interests of citizens, legal entities or other organizations, and ensure national security and public interests. The Decision has the same legal effect as a law.

DEFINITION OF PERSONAL DATA

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

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

DEFINITION OF SENSITIVE PERSONAL DATA

There is currently no definition of "sensitive personal data" within existing or proposed laws or regulations.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

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

REGISTRATION

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

DATA PROTECTION OFFICERS

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

COLLECTION AND PROCESSING

Under the Draft Guidelines, data controllers may collect and process personal data when the following conditions are met:

- laws and regulations explicitly authorise such collection or the data subject consents; and
- the data controller has a specific, clear and reasonable purpose for doing so.

Before a data controller collects personal data, it should notify the data subject of the following:

- the purpose, the scope of use and collection methods related to the collecting of the personal data;
- the name, address and contact information of the data controller;
- the consequences of not providing the requested personal data;
- the rights of the data subject; and
- channels for submitting complaints.

Data controllers are not allowed to collect personal data that has no direct relation with the stated purpose, and in particular data relating to race, religion, DNA, fingerprints, physical condition or sex life.

The data controller should process personal data for the stated purpose and within the scope that the data controller has notified to the data subject. The data controller should take measures to keep the collected personal data confidential during processing and storage of the data. If the data controller uses a third party to process the personal data, they should inform the data subject of this fact prior to collecting the data.

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

- comply with the lawful, reasonable, necessary principle;
- specify the purpose, method and scope regarding the collection and use of the citizen's personal information;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the personal information subject consents;
- satisfy the requirements established by the laws, regulations and mutual agreement; and
- disclose the rules regarding collection and use.

TRANSFER

Under the Draft Guidelines, data controllers may transfer personal data to third parties (group companies are considered third parties) if the following conditions are met:

- the data controller explains the purpose and subject of the data transfer to the data subject;
- the data subject explicitly consents to such transfer; and
- the data controller ensures the receiver has the capability to properly process the personal data and that the personal data will be safe during the transfer.

With respect to transfers, there are no specified requirements in the Decision.

SECURITY

Under the Draft Guidelines, data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorised or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data.

Article 4 of the Decision has the same requirements as noted above.

BREACH NOTIFICATION

There is no mandatory requirement in PRC law to report data security breaches or losses to any authority or to data subjects.

ENFORCEMENT

According to Articles 9 and 11 of the Decision, failure to comply with these requirements established in the Decision is an offence. Supervisory authorities can take considerable measures to punish or stop these illegal behaviours. Network service providers should cooperate and provide technical support when supervisory authorities perform their duties.

There is no enforcement provision or applicable penalties for non compliance with personal data protection requirements under other PRC laws and regulations.

ELECTRONIC MARKETING

Under the Decision, any organizations and individuals are forbidden from acquiring personal electronic information by theft or other illegal methods. Also, they are proscribed from selling or unlawfully providing personal electronic information to anyone else.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Network service providers will require users to provide genuine identification information when signing agreements to grant them access to the Internet, fixed-line telephone or mobile phone services or to permit users to make information publicly.

The Decision prohibits any organizations and personnel from sending commercial electronic information to a personal fixed-line telephone, mobile phone or email address without the consent or request of electronic information recipient, or where the recipient has explicitly declined to receive such information.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The Decision indicates that network service providers and other companies should ensure the privacy of personal information. They are not allowed to disclose, falsify, damage, as well as sell or unlawfully provide personal electronic information to anyone else.

Article 5 of the Decision indicates that network service providers should strengthen management of information issued by users. Also, network service providers should stop the transmission of unlawful information and take necessary measures to remove them and save relevant records, then report to supervisory authorities.

Once citizens find network information that discloses their identity or breaches their legal rights, or are harassed by commercial electronic information, they have the right to require that the network service provider delete related information or take measures to prevent such behaviours.

There are specific requirements regarding cookies and location data within existing laws or regulations in the PRC.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

10. COLOMBIA

CONTRIBUTION DETAILS

Gómez-Pinzón Zuleta Abogados S.A.
Calle 67 No. 7-35
Oficina 1204
Bogotá D.C., Colombia
www.gpzlegal.com

Santiago Jaramillo Caro
Socio – Partner
T +57 1.319.2900, ext. 903
sjaramillo@gpzlegal.com

LAW

Article 15 of the Colombian Constitution sets forth fundamental rights to intimacy, good name or reputation and data protection.

Law 1266/08 ("**Law 1266**"), reviewed by the Colombian Constitutional Court in Decision C 1011/08, regulates the collection, use and transfer of personal information regarding monetary obligations related to credit, financial and banking services.

Law 1581 of 2012 ("**Law 1581**"), reviewed by the Colombian Constitutional Court in Decision C-748/11, contains comprehensive personal data protection regulations. This law is intended to implement the constitutional right to know, update and rectify information gathered about them in databases or files, enshrined in Article 20 of the Constitution, as well as other rights, liberties and constitutional guarantees referred to in Article 15 of the Constitution.

Accordingly Law 1581 applies to: (i) personal data stored in any public or private database or files; (ii) any treatment of personal data in Colombia; and (iii) operations performed by individuals who are not located in Colombia but are subject to the jurisdiction of Colombian Law under international standards and treaties.

Under Law 1581, the data owner (data subject) must always give prior, express and informed consent for all activities pertaining the collection, use and transfer of personal data, except those that are specifically exempted from all or part of the Law, which includes the processing of credit data under Law 1266.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF PERSONAL DATA

Law 1266 defines "personal data" as any information related to one or several identified or identifiable persons or which can be associated with an individual or a legal entity. Personal data may be public, semi private or private. Semi private data is data that is not deemed private, sensitive or public.

Under Law 1581, the definition of "personal data" specifically includes information related to or that may be related to one or several identified or identifiable natural or legal persons.

DEFINITION OF SENSITIVE PERSONAL DATA

Under Law 1266 "private data" is data that, due to its sensitive or confidential nature, is relevant only to the data owner. For example, data that pertains to the right to intimacy may be deemed sensitive data under Colombian law.

Under Law 1581 "sensitive data" is data that relates to the intimacy of the data owner, or that, if disclosed without consent, could lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, trade-union membership, social organizations, human rights organizations, or those organizations that promote the interests of any political party or that ensure the rights and guarantees of opposition political parties, as well as data relating to health, sexual life and biometrics.

NATIONAL DATA PROTECTION AUTHORITY

Two different governmental authorities were designated as data protection authorities by Law 1266: The Superintendency of Industry and Commerce ("**SIC**") and the Superintendency of Finance ("**SFC**"). As a general rule, the SIC will be the data protection authority, unless the administrator of the data is a company that performs financial or credit activities under oversight of the SFC as set forth in applicable law, in which case the SFC will also serve as a data protection authority.

The SIC is the sole data protection authority responsible for monitoring compliance with the principles, rights, guarantees and procedures provided under Law 1581.

REGISTRATION

Law 1581 created the National Register of Databases as a public directory of all databases operating in the country. This Register will be managed by the SIC, and may be consulted by any citizen.

DATA PROTECTION OFFICERS

Neither Laws 1266 nor 1581 require organisations to appoint a data protection officer. However, data processors and data controllers are obliged to maintain adequate security levels for the protection of databases, as well as an administrative infrastructure to respond to data owner's requests and claims.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

Under Law 1266 and Decision C 1011, as a general rule the collection and cross border transfer of Private and Semi private Data can be performed only with the prior consent of the data owner unless an exception applies. The exceptions, set forth in Article 5 of Law 1266, permit personal data to be disclosed or delivered directly, without consent, to the following and in the following conditions:

- To the data owner or to a person to whom the owner has authorised such disclosure;
- To data users;
- To any judicial authority, pursuant to a judicial order;
- To Government Agencies or entities, when the data is required for the performance of legal or constitutional functions;
- To the Administrative Authorities who require such data for disciplinary, fiscal or administrative investigations; or
- To other databases that have the same purpose as the one of the disclosing data processor (*but see* Decision C 1011 below) or to databases as authorised by the data owner.

Under the interpretation in Decision C 1011, the Private and Semi Private Data of data owners may be disclosed in the foregoing cases, if the following conditions are observed:

- Except for the disclosure to the data owner, judicial authorities, governmental agencies, and administrative authorities, the disclosure can be performed only if the data owner gives his or her prior consent; or
- When the data is delivered to governmental agencies, they will be deemed to act as data users and will have all the corresponding obligations which include those pertaining to confidentiality, restricted circulation, and security of data.

Similar to Law 1266, according to article 10 of Law 1581, any operation performed on personal data requires the prior, express and informed consent from the data owner except in the following cases:

- Data required by a public or administrative agency in performance of their duties or required by a court order;
- Data that it is deemed public data;
- Data related to medical emergencies;
- Data related to historical, statistical or scientific purposes; and
- Data related to the Civil Registration of Persons.

Similarly, article 13 states that personal data can be disclosed without consent to the following:

- To the data owners, their successors or their legal representatives;
- To any administrative authority, when the data is required for the performance of public duties, or pursuant to a judicial order; or
- To third persons to whom the owner has authorised such disclosure, or who are authorised by law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

INTERNATIONAL TRANSFER

Under Law 1581, the cross border transfer of data is prohibited unless the foreign country where the data will be transferred meets at least the same data protection standards as the ones provided under Colombian law. This prohibition also applies to personal data governed by Law 1266.

Adequate levels of data protection will be determined in accordance with the standards set by the Data Protection Authority.

This prohibition against cross-border transfers does not apply in the following cases:

- If the data owner has expressly and unambiguously authorised the cross-border transfer of data (notice of specific elements, including destination and usage, must be given for consent to be effective);
- Exchange of medical data;
- Bank transfers and stock;
- Transfers agreed under international treaties to which the Colombia is a party;
- Transfers necessary for the performance of a contract between the data owner and the controller, or for the implementation of pre-contractual measures provided there is consent of the owner; and
- Transfers legally required in order to safeguard the public interest.

SECURITY

As mentioned, Law 1266 provides that data processors must implement security systems with technical safeguards to ensure the safety and accuracy of the data, and to prevent damage, loss, and unauthorised use or access of the data.

Similarly, Law 1581 requires that data protection processors and controllers implement the necessary technical, physical, and administrative safeguards to ensure the safety of databases and to prevent their damage, loss, and unauthorised use or access.

BREACH NOTIFICATION

Article 17-N of Law 1581 requires notice to the DPA of certain security risks or violations of security policies related to the management of personal data. Other than this obligation, currently there are no specific breach notification regulations in Colombia.

ENFORCEMENT

Data Protection Authorities are allowed to initiate administrative investigations against those who breach the provisions of Laws 1266 or Law 1581 and impose penalties of up to 2,000 Minimum Monthly Legal Wages (approx. US$670.000) for each case, and sanctions that include the temporary or permanent closure of the professional or commercial activities of the subject who breached the data protection regime.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The penalties under Law 1581 only apply to private persons. If an offense is committed by a public authority, the SIC shall refer the action to the Attorney General's Office to initiate the respective investigation.

Additionally, on 5 January 2009 Colombia's Congress enacted Act 1273, which added an "Information and Data Protection" criminal offence to Colombia's Criminal Code. In particular, Article 269F states: "Violation of Personal Data: Anyone who, without being authorised to do so, to its own benefit or for a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or uses personal codes, personal data contained in files, archives, databases or similar means, will be held liable for imprisonment for a term of forty eight (48) to ninety six (96) months and a fine."

Finally, data owners have the right to file, before any Colombian judge, a special constitutional action "Acción de Tutela" (Constitutional Writ of Protection) to have their fundamental right to privacy, data protection or habeas data protected. This Constitutional Writ of Protection involves a preferential and summary proceeding under which the pertinent court must issue a decision within the 10 days following the date on which the action is filed. This means that in those cases in which the right to privacy, to intimacy or to habeas data is affected, an expeditious action could be implemented to protect the fundamental rights of the individual. In this regard, Decree 2591/91 expressly provides that an Acción de Tutela can be filed against a private individual or company that violates Article 15 of the Colombian Constitution.

In general terms, a court granting an Acción de Tutela that involves habeas data will issue a decision ordering that data be rectified, updated or deleted. Failing to observe a Court's ruling could result in an imprisonment order against the defendant for a period up to 10 days.

ELECTRONIC MARKETING

Electronic Marketing is regulated by Law 527/99. The general rule is that opt-in consent from a data subject is required in order to send electronic marketing materials.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

In general, consent is required to use cookies and other tracking mechanisms to collect any data that could be used to identify an individual; consent may generally be obtained via the user's acceptance to the privacy policy if the use of cookies (and the way to disable them) is fully disclosed in the privacy policy. IP address may be considered personal data; however, currently there is no official opinion or law addressing whether IP address is personal information.

Also, under the principle of access and restricted delivery enshrined in Article 4 of Law 1581, personal data may not be available on the Internet or in other mass media, unless the access is technically controllable to ensure access is available only to data owners or authorised third parties. This prohibition applies unless the information is public data, in which case its disclosure and circulation is possible within the limits established by law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

11. COSTA RICA

CONTRIBUTION DETAILS

FACIO & CAÑAS
Apdo. Postal 5173-1000
San José, Costa Rica
www.fayca.com

Carlos J. Oreamuno
Partner
T +(506) 2233 9202
F +(506) 2255-2510
coreamuno@fayca.com

Alexander Araya
Partner
T +(506) 2256-5555 ext. 712
F +(506) 2255-2510
aaraya@fayca.com

LAW

The development of data privacy regulation in Costa Rica is divided among two laws. The first law is Law No. 7975, Undisclosed Information Law, which makes it a crime to disclose confidential/personal information without authorization. The second law is Law No. 8968, Protection in the Handling of the Personal Data of Individuals, which was enacted to regulate the activities of companies that administer databases containing personal information. Therefore, its scope is limited.

DEFINITION OF PERSONAL DATA

Personal information contained in public or private registries (e.g. medical records) that identifies or could be used to identify a natural person. Personal information can only be disclosed to persons/entities with a "need to know" such information.

DEFINITION OF SENSITIVE PERSONAL DATA

Personal information relating to ideological orientation, creed, sexual preferences. Sensitive personal data cannot be disclosed without express prior authorization from the data subject.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to Law No. 8968, the Agency for the Protection of Individual's Data, hereinafter the "Agency" is the entity charged with enforcing compliance with the regulation. The Constitutional Court also has jurisdiction to hear claims alleging violations of the Laws.

REGISTRATION

Under Law 8968, companies that manage databases containing personal information and that sell such personal information must register with the Agency.

DATA PROTECTION OFFICERS

There is no requirement for a data protection officer.

COLLECTION AND PROCESSING

Any company may store and manage a database containing personal information if the following rules are respected: (i) when accumulating personal information, private companies and/or the government must respect the "sphere of privacy" to which all individuals are entitled; (ii) companies that maintain personal information about others in their databases must ensure that such information is (a) materially truthful; (b) complete; (c) accurate; and, (d) individuals have access to their personal data and must be entitled to dispute any erroneous or misleading information about them.

Companies that manage databases containing personal information and that sell such personal information must comply with Law 8968, including by (i) reporting the company and the database to the Agency, (ii) reporting the technical issues related to the security of the database, (iii) protecting and respecting confidentiality issues, (iv) securing the information they maintain, and (v) establishing a proceeding to review requests by individuals to review and amend any error or mistakes in the database.

TRANSFER

Transfer of personal information is authorised if: (i) data subjects give written consent; or (ii) information transferred is public.

SECURITY

Any company or individual using and/or managing this type of information must take all necessary steps to guarantee that the information is kept in a safe environment. If security is breached because of improper management or protection, then the responsible company may be held liable, and may be subject to penalties and civil liability for any harm.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

There is no mandatory requirement. Nonetheless, if there is a breach the entity is liable.

ENFORCEMENT

All claims can be brought directly to: (i) the entity, (ii) the Agency or (iii) the Constitutional Court.

ELECTRONIC MARKETING

General rules of data protection will apply. There is little to no regulation of electronic marketing. However, pursuant to the Telecommunications Act, marketing companies may not advertise via phone unless they have express written consent from the data subject.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There has been little to no regulation in this area. However, the general rules of data protection issued by the Constitutional Court, with respect to the collection and processing of personal information, do apply.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

12. CYPRUS

CONTRIBUTION DETAILS

Pamboridis LLC
www.pamboridis.com

Christy Spyrou
Senior Associate
T +357 22 752525
spyrou@pamboridis.com

LAW

Cyprus implemented the EU Data Protection Directive 95/46/EC in November 2001 with the Processing of Personal Data (Protection of the Individual) Law of 2001 and its amendments (Law No. 37(I)/2003, 105(I)/2012)).

DEFINITION OF PERSONAL DATA

"Personal data" or "data" means any information relating to a living data subject. Consolidated data of a statistical nature, from which the data subject cannot be identified, is not deemed to be personal data.

DEFINITION OF SENSITIVE PERSONAL DATA

"Sensitive data" means data concerning racial or ethnic origin, political convictions, religious or philosophical beliefs, participation in a body, association and trade union, health, sex life and erotic orientation as well as data relevant to criminal prosecutions or convictions.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Commissioner for Personal Data Protection ("**Commissioner**")
1, Iasonos Str. 2nd Floor, 1082 Nicosia, Cyprus
P.O. BOX 23378, 1682 Nicosia
T 0035722818456
F 0035722304565
commissioner@dataprotection.gov.cy

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

Data controllers or data protection officers who process personal data must notify the Commissioner in writing about the establishment and operation of a filing system or the commencement of processing of personal data. The information provided in this written notice is then filed in the Register of Filing Systems and Processing kept by the Commissioner and any change to this information must be notified in writing without delay by the data controller or data protection officer to the Commissioner.

The notification should include the following information:

- the full name, business name or title and address of the data controller;
- the address where the filing system is established or the main equipment necessary for the processing to be installed;
- a description of the purpose of the processing of the personal data;
- the categories of data subjects;
- the categories of data which are or are intended to be processed;
- the period of time for which the data will be processed or the filing system will be established;
- the recipients to whom the data will be communicated;
- the proposed transmissions of data to third countries and the purpose thereof; and
- the basic characteristics of the system and the measures for the security of the filing system or of the processing.

DATA PROTECTION OFFICERS

The law provides that any organisation that processes personal data must designate to the Commissioner a controller or data protection officer who is ultimately responsible for the processing of personal data.

COLLECTION AND PROCESSING

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

- the data subject consents;
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party;
- the processing satisfies the data controller's legal obligation;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the processing protects the data controller's vital interests;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller or a third party to whom the data will be communicated; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the personal data is communicated, on condition that such interests override the rights, interests and fundamental freedoms of the data subjects.

Processing of sensitive personal data is permitted when the data subject has given his explicit consent or when one or more of a list of more stringent conditions are fulfilled.

TRANSFER

Data controllers may transfer personal data out of the European Economic Area only after the data protection officer or controller has obtained a license for such transfer from the Commissioner. The Commissioner shall issue the licence only if he considers that the said country ensures an adequate level of protection.

The transmission of personal data to a country which does not ensure an adequate level of protection, is permitted exceptionally after a licence of the Commissioner where one or more of the following conditions are fulfilled:

- the data subject consents;
- the transmission is necessary in order to protect the vital interests of the data subject;
- the transmission is necessary for the conclusion and performance of a contract to which the data subject is a party;
- the transmission is necessary for the implementation of pre contractual measures which have been taken in response to the data subject's request;
- the transmission is necessary in order to safeguard a superior public interest;
- the transmission is necessary for the establishment, exercise or defence of legal claims before a court; or
- the transmission is made from a public register which, according to the law, provides information to the public or to any person who can show legitimate interest.

SECURITY

The processing of data is confidential. It shall be conducted solely by persons acting under the authority of the data controller or the processor and only after their instructions.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Data controllers must take the appropriate technical and organisational measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures must ensure a level of security which is appropriate to the risks involved in the processing of the data.

From time to time, the Commissioner gives directions with regard to the degree of security of the data and to the measures of protection required to be taken for every category of data, also taking into account technological developments.

If the processing is performed by the processor, the assignment for the processing must be made in writing. The assignment must provide that the processor shall perform the processing only upon instructions from the controller and that the remaining obligations set out in the relevant sections of the Processing of Personal Data Law shall also lie on the processor.

BREACH NOTIFICATION

There is no mandatory requirement in the Processing of Personal Data Law to report data security breaches or losses to the Commissioner or to data subjects.

ENFORCEMENT

The Commissioner is responsible for the enforcement of the processing of personal data law.

The Commissioner may impose on the data controller or data protection officer or their representatives the following administrative sanctions:

- a fine of up to EUR 30,000;
- a temporary revocation of licensc;
- a permanent revocation of licence;
- a warning with a specific time limit for the termination of the contravention; or
- the destruction of the filing system or the cessation of processing and the destruction of the relevant data.

Section 26 (1) of the Processing of Personal Data Law lists the breaches of the law which constitute an offence and the penalties imposed. Such penalties range from imprisonment for a term not exceeding three years or a fine up to approximately EUR 5,130 or both, to imprisonment for a term not exceeding five years or a fine up to EUR 8,453 or both, depending on whether:

- the offence was caused by negligence;
- the person committing the offence intended to obtain for himself or anyone else an unlawful financial benefit or cause injury to a third party; or
- the committed offence endangered the free functioning of the Government of the Republic or national security.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The offences committed in contravention of the provisions of this section 26 (1) for which no other penalty is expressly provided, are punishable with imprisonment for a term not exceeding one year or with a fine not exceeding approximately EUR 3,417.20 or by both such imprisonment and fine.

ELECTRONIC MARKETING

The Regulation of Electronic Communications and Postal Services Law of 2004 (112(I)/2004) as amended by Law No 105(I)/2012 ("**Electronic and Postal Services Law**") will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an e-mail address is likely to be personal data for the purposes of the Electronic and Postal Services Law).

Section 106 of the Electronic Communications and Postal Services Law states the following:

- the use of automatic calling machines, fax, or electronic mail, or SMS messages, for the purposes of direct marketing, may only be allowed in respect to subscribers who have given their prior consent;
- unsolicited communications for the purposes of direct marketing, by means other than those referred to in (i) above, are not allowed without the consent of the subscribers concerned;
- the rights referred to in (i) and (ii) above shall apply to subscribers who are natural persons. The Commissioner of Electronic Communications and Postal Regulation, may, after consultation with the Personal Data Commissioner, issue an order to safeguard that legitimate interests of legal persons, regarding unsolicited communications, are adequately protected;
- notwithstanding (i) above, in cases where a natural or legal person obtains from its customers contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic details for direct marketing of its own similar products or services, provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use; and
- electronic mail sent for direct marketing must not disguise or conceal the identity of the sender or the person on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Part 14 of the Electronic and Postal Services Law deals with the collection of location and traffic data and use of cookies (and similar technologies) by publically available electronic communication service providers.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Traffic Data – Traffic Data concerning subscribers and users, which are submitted to processing so as to establish communications and which are stored by Organisations, shall be erased or made anonymous at the end of a call, except: for the purpose of subscriber billing and interconnection payments; and if the subscriber or user consent that the data may be processed from an undertaking for the purpose of commercial promotion of the services of electronic communications of the latter or for the provision of added value services.

The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information. Users or subscribers shall be given the possibility to withdraw their consent for the processing of Traffic Data at any time.

Location Data – Location Data may only be processed when made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

The service provider must inform the users or subscribers, prior to obtaining their consent, of the following:

- type of Location Data which will be processed;
- the purpose and duration of the processing; and
- whether the data will be transmitted to a third party for the purpose of providing the value added service.

Users or subscribers shall be given the possibility to withdraw their consent for the processing of Location Data at any time.

Cookie Compliance – The storage and use of cookies and similar technologies is permitted only if the subscriber or user concerned has been provided with clear and comprehensive information, *inter alia*, about the purposes of the processing, and has given his consent in accordance with the Processing of Personal Data Law.

The above shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

13. CZECH REPUBLIC

CONTRIBUTION DETAILS

Eva Ruhswurmová
Senior Associate
T +420 222 817 802
eva.ruhswurmova@dlapiper.com

LAW

The regulation of personal data protection in the Czech Republic is based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "**Data Protection Directive**"). The main provisions are contained in the Act no. 101/2000 Coll., on the Protection of Personal Data, as amended ("**Act**").

DEFINITION OF PERSONAL DATA

Personal data means any information relating to an identified or identifiable data subject. A data subject shall be considered identified or identifiable if it is possible to identify the data subject directly or indirectly in particular on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychical, economic, cultural or social identity.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive data means personal data revealing nationality, racial or ethnic origin, political attitudes, trade union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sexual life of the data subject, as well as any genetic or biometric data of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The Office for Personal Data Protection ("**Office**")Pplk. Sochora 27
170 00 Prague 7
Czech Republic
T +420 234 665 111
T +420 234 665 555
F +420 234 665 444
posta@uoou.cz
www.uoou.cz

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

Whoever intends to process personal data as a data controller (or change the already registered processing), shall be obliged to notify this fact in writing to the Office prior to commencing personal data processing (or change of data processing).

The notification must include at least the following information:

- identification details of the data controller (business name, seat and identification number, and name of persons who are statutory representatives of the data controller);
- purpose of processing;
- categories of data subjects and of personal data;
- sources of personal data;
- description of the manner of personal data processing;
- location or locations of personal data processing;
- recipient or category of recipients of personal data;
- anticipated personal data transfers to other countries; and
- description of measures adopted for ensuring the protection of personal data.

If the notification including all required information is accepted by the Office, personal data processing may be started by a data controller after the expiration of 30 days from the delivery of the notification to the Office. In such case the Office records the information stated in the notification in the register of data controllers.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer stipulated by the Act.

COLLECTION AND PROCESSING

The unequivocal (and revocable) consent of a data subject is required for the processing of personal data. Written consent is not required. However, it is recommended to obtain consent in writing, since the data controller must be able to prove the consent of a data subject during the whole period of the data processing.

Before the consent of the data subject is granted, the data subject must be clearly informed about all the aspects of processing of their personal data.

Personal data may be collected only for processing, or to be processed, if it is adequate, relevant and not excessive in relation to specific purposes for which the data is collected. Personal data may not be used for purposes which are incompatible with the reasons for which the data has been collected.

Personal data collected for different purposes may not be merged.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Personal data must be accurate and maintained up to date and it must accurately reflect the current situation of the data subject. Partially or wholly inaccurate data must be deleted or corrected.

The data controller or data processor must not disclose the personal data of the data subject to any third party without the consent of the data subject except where required or allowed to do so by law.

The personal data must be deleted once it ceases to be necessary or relevant for the purposes for which it was collected. However, where a specific law (e.g. the Archiving Act) sets an obligation on the data controller or data processor to keep personal data for a specific period of time, such data may not be deleted even if the data is no longer needed for the purpose for which it has been collected and processed.

Personal data must be stored in a format which permits the data subject to exercise their rights of access, rectification, cancellation and opposition.

Special protection rules apply in the case of processing certain "sensitive data" relating to ideology, religion, beliefs, trade union membership (this data often appears on the payroll), racial origin, health (e.g. disability, time off work due to illness, maternity leave, etc.) and sex life. Special care is required when collecting and processing such data. Express informed consent is generally required for the collection, processing and transfer of such data.

Since 1 January 2006 special protection rules also apply for the processing of birth numbers. Birth numbers (a 10 digit number sequence containing information about date of birth and sex of the holder) are widely used by businesses as key identifiers (of customers, employees etc.) in databases because they provide unambiguous identification of all Czech citizens. Data controllers need the express consent of data subjects before processing their birth numbers.

TRANSFER

There is a free flow of personal data guaranteed by the Act if personal data is transferred to a member state of the European Union.

As for personal data transfer to other countries, the Act distinguishes several different groups of data transfers.

In the first group, the Act stipulates that personal data may be transferred to other countries if the prohibition to restrict free movement of personal data ensues from an international treaty, the ratification of which was approved by the Parliament and which is binding for the Czech Republic. A typical example of such treaty is the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

In the second group, a personal data transfer is possible on the basis of a decision of an institution of the European Union, for example Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, or *Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe*

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

harbour privacy principles and related frequently asked questions issued by the US Department of Commerce regarding subjects of the Safe Harbour by the US Department of Commerce. It should be noted that not every American or Canadian subject is covered by the aforementioned decision.

There are also European decisions providing that personal data may be transferred without official approval under the condition that the contract includes certain standard contractual clauses set by those decisions. These decisions are for example *Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, Commission Decision amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries or Commission Decision on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.*

Neither of the above described ways of transfer of personal data is subjected to an official approval.

In cases other than the two above described ways of transfer of personal data, controllers shall seek a prior permission of the Office to the transfer. For this purpose the controller must prove that:

- the data transfer is carried out with the consent of, or on the basis of an instruction by the data subject;
- in a third party country, where personal data is to be processed, sufficient specific guarantee for personal data protection have been created;
- the personal data concerned is part of a publicly accessible data file on the basis of a special Act or, on the basis of a special Act accessible to someone who proves they have a legal interest;
- 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 or change of a contract, carried out by the data subject, or for the performance of a contract to which the data subject is a contracting party;
- the transfer is necessary to perform a contract between the controller and a third party, concluded in the interest of the data subject, or to exercise other legal claims; or
- the transfer is necessary for the protection of rights or important vital interests of the data subject, in particular for saving lives or providing health care.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

The controller and the processor are obliged to adopt measures preventing unauthorised or accidental access to personal data, its alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data. This obligation remains valid also after termination of personal data processing.

The controller and the processor are also obliged to develop and to document the technical organisational measures adopted and implemented in order to ensure personal data protection in accordance with the Act and other legal regulations.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the Office or to data subjects.

ENFORCEMENT

Both data controllers and data processors are potentially liable for any breach of the Act. In case of a breach of the Act, the Office may order measures to be adopted and impose fines. The Office may impose fines of up to 5 million CZK (approx. EUR 175,000). Fines of up to 10 million CZK (approx. EUR 350,000) may be imposed if:

- a substantial number of persons are jeopardised by unauthorised interference in their private and personal life; or
- obligations relating to the processing of sensitive data are breached.

A data subject who considers that there has been personal data processing in breach of the Act is entitled to complain directly to the Office.

ELECTRONIC MARKETING

When dealing with e-marketing, it is necessary to bear in mind that it is quite strictly regulated in terms of Act No. 480/2004 Col. on Some Services of Information Agencies ("**ASSIA**") as well as other previously mentioned regulations (esp. the Data Protection Directive and the Act).

The ASSIA states that before sending an e-mail containing marketing information, the consent of the receiver must be obtained. Furthermore, each such message must contain clear and visible information that any further sending of such e-mails can be rejected by the receiver together with the sender's contact information and information on under whos name the e-mail is being sent. Last but not least, each such e-mail must contain information that it is a commercial message.

In order to maintain e-marketing as an effective tool, its provider should operate with good-quality databases, which enable a direct targeting of the relevant message. When processing personal data for marketing databases, it is necessary to abide strictly by the Act. All rules described above apply to e-marketing respectively.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Online privacy is supervised by the Office. Handling personal data is subject to the similar rules as mentioned above and specific areas are governed by Act No. 127/2005 Coll. on Electronic Communications ("**AEC**").

Consent to collection and processing of personal data means the consent is made by electronic means (especially by filling in an electronic form).

Public electronic communication service providers are obliged to ensure the security of the personal data they process which includes technical security and creation of internal organizational regulations.

In cases of a breach of the protection of the personal data of an individual, a public electronic communication service provider is obliged to notify the Office, and in the event that breach of protection is capable of affecting privacy of an individual in a serious way, the individual must be notified.

Apart from a few exceptions, traffic data held by a public electronic communication service provider must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication.

As regards cookies, the Czech law is still using the "opt-out" principle (the user must be informed and explicitly allowed to refuse the cookies storage). The "opt-in" principle as introduced by the Directive 2009/136/EC has not implemented into the Czech law.

Relevant supervising and enforcing authorities in this area are primarily the Office and to some extent also the Czech Telecommunication Office.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

14. DENMARK

CONTRIBUTION DETAILS

Horten Lawfirm
www.horten.dk

Egil Husum
Senior Associate
T +45 5234 4224
ehu@horten.dk

LAW

Denmark implemented the EU Data Protection Directive 95/46/EC in June 2000 with the Act on Processing of Personal Data ("**Act**").

DEFINITION OF PERSONAL DATA

Any information relating to an identified or identifiable natural person (data subject).

DEFINITION OF SENSITIVE PERSONAL DATA

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life.

NATIONAL DATA PROTECTION AUTHORITY

Datatilsynet ("**DPA**")
Borgergade 28, 5
DK 1300 København K
T +45 3319 3200
F +45 3319 3218

REGISTRATION

Unlike most EU Member States, Denmark does not require a general registration of controllers, processing activities or databases with personal information.

However, data processors established in Denmark who offer electronic processing services must, prior to the commencement of such processing operations, notify the DPA.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Besides this notification requirement, processing of personal data must be notified by the controller to the DPA if the processing includes sensitive or other purely private data. Such a registration should include the following information:

- the name and address of the controller, his representative (if any) and the processor (if any);
- the category of processing and its purpose;
- a general description of the processing;
- a description of the categories of data subjects and of the categories of data relating to them;
- the recipients or categories of recipients to whom the data may be disclosed;
- intended transfers of data to third countries;
- a general description of the measures taken to ensure security of processing;
- the date of the commencement of the processing; and
- the date of deletion of the data.

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

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

- the data subject has given his explicit consent; or
- 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; or
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data is disclosed, and these interests are not overridden by the interests of the data subject.

Sensitive personal data (as detailed above) may be processed only if:

- the data subject has given his explicit consent to the processing of such data;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

Personal data about purely private matters, including data about criminal offences and serious social problems, may be processed only if:

- the data subject has given his explicit consent to such disclosure;
- disclosure takes place for the purpose of pursuing private or public interests which clearly override the interests of secrecy, including the interests of the person to whom the data relate;
- disclosure is necessary for the performance of the activities of an authority or required for a decision to be made by that authority; or
- disclosure is necessary for the performance of tasks for an official authority by a person or a company.

Furthermore, the data controller must provide the data subject with the necessary information to fulfil the duty of information, including information about the identity of the controller and the purposes of the processing for which the data is intended and any further information which is necessary having regard to the specific circumstances in which the personal data is collected and/or obtained.

TRANSFER

Data controllers may transfer personal data out of the European Economic Area ("**EEA**") (insecure third country) if any of the following conditions are met:

- the data subject has given his explicit consent;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;
- the transfer is necessary for the prevention, investigation and prosecution of criminal offences and the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the transfer is necessary to safeguard public security, the defence of the realm, or national security.

Furthermore, data controllers may transfer personal data out of the EEA, if the transfer is based on the Safe Harbor programme (to the USA) or the data exporter and the data importer has entered into standard contractual clauses approved by the EU Commission and these clauses have not been amended.

The DPA may authorise a transfer of personal data to an insecure third country where the controller adduces adequate safeguards with respect to the protection of the rights of the data subject.

SECURITY

Data controllers must implement appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down in the Act. The same applies to data processors.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the DPA. However, DPA practice stresses that affected data subjects normally should be informed about breaches.

ENFORCEMENT

The DPA, which consists of a Council and a Secretary, is responsible for the supervision of all processing operations covered by the Act. If the DPA becomes aware that a data controller is in breach of the Act, the DPA can state their legal opinion.

Furthermore, the DPA can impose fines and a person who violates the Act is liable to a prison sentence of up to four months.

In addition to this, a controller shall compensate for any damage caused by the processing of personal data in violation of the Act.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be "personal data" for the purposes of the Act). A company can process data concerning existing customers for marketing of the company's own products if the processing is necessary for the purposes of the legitimate interests pursued by the company and these interests are not overridden by the interests of the consumer. Besides that, processing of personal data for marketing purposes normally requires consent.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

According to the Danish Marketing Practices Act, a trader must not approach anyone by means of electronic mail, an automated calling system or facsimile machine with a view to the sale of products, real property, other property, labour and services unless the party concerned has requested him to do so. If a trader that has received a customer's electronic contact details in connection with the sale of products or services, he may market his own similar products or services to that customer by electronic mail, provided that the customer has the option, free of charge and in an easy manner, of declining this both when giving his contact details to the trader and in the event of subsequent communications.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Directive 2009/136/EC was implemented in the new Danish Act on Electronic Communications Services and Networks which came into force on 25 May 2011 in accordance with the implementation deadline in the Directive.

According to the "Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-user Terminal Equipment", which came into force on 14 December 2011, the use of cookies requires consent. The consent must be freely given and specific. However, this does not imply that consent must be obtained each time a cookie is used but a user must be given an option. Furthermore, the consent must be informed which implies that a user must receive information about the consequences of consenting. Finally, the consent must be an informed indication of the user's wishes. Normally, consent is obtained through tick-the-box but also the use of a homepage after having received the relevant information concerning cookies can constitute consent. Yet, consent by use of a homepage must be used with caution.

In addition to this, the information to the user must fulfil the below mentioned requirements: (i) The information must be clear and easy to understand; (ii) the purpose of the use of the cookies must be provided; (iii) the identity of the person or entity which is responsible for the use of the cookies must appear; (iv) the possibility of withdrawal of consent must be easily accessible and be described in the information; and (v) this information must be easily accessible for the user at all times.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

15. DUBAI INTERNATIONAL FINANCIAL CENTRE (DIFC)

CONTRIBUTION DETAILS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Ken Dearsley
Senior Counsel
T +971 4 438 6286
ken.dearsley@dlapiper.com

Jamie Ryder
Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

Robert Flaws
Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR, for organisations to appoint a data protection officer, though note the general obligation of a Data Controller to implement appropriate technical and organisational measures to protect Personal Data, as further detailed below (see Security section below).

In addition, where Processing of Personal Data or Sensitive Personal Data is carried out on a Data Controller's behalf, the Data Controller must choose a "Data Processor" providing sufficient guarantees in respect of the technical security measures and organisational measures governing the Processing to be carried out, and must ensure compliance with those measures (Article 16(3)).

COLLECTION AND PROCESSING

Data Controllers may collect and process Personal Data when any of the following conditions are met:

- the Data Subject has given his/her written consent to the Processing of that Personal Data (Article 9(1)(a));

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- 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 (Article 9(1)(b));
- Processing is necessary for compliance with any legal obligation to which the Data Controller is subject (Article 9(1)(c));
- Processing is necessary in order to protect the vital interests of the Data Subject (Article 10.1(c));
- Processing is necessary for the performance of a task carried out in the interests of the DIFC, the Dubai Financial Services Authority, the DIFC Court or in the exercise of the DPC's functions or powers vested in the Data Controller or in a third party to whom the Personal Data are disclosed (Article 9(1)(d)); or
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the third party or parties to whom the Personal Data is disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation (Article 9(1)(e)).

TRANSFER

Data Controllers may transfer Personal Data out of the DIFC if the Personal Data is being transferred to a Recipient in a jurisdiction that has laws that ensure an adequate level of protection for that Personal Data (Article 11(1)(a)). An adequate level of protection is when the level of protection in that jurisdiction is acceptable pursuant to the DPR or any other jurisdiction approved by the DPC (Article 11(2)).

In the absence of an adequate level of protection, Data Controllers may transfer Personal Data out of the DIFC if the:

- DPC or his/her delegate has granted a permit or written authorisation for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of this Personal Data (Article 12(1)(a)). Article 5.1 of the DPR then sets out the requirements for applying for such a permit (including a description of the proposed transfer of Personal Data for which the permit is being sought and including a description of the nature of the Personal Data involved);
- Data Subject has given his/her written consent to the proposed transfer (Article 12(1)(b));
- transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request (Article 12(1)(c));
- transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a third party (Article 12.1(d));
- transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims (Article 12.1(e));

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- transfer is necessary in order to protect the vital interests of the Data Subject (Article 12.1(f));
- transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case (Article 12(1)(g));
- transfer is necessary for compliance with any legal obligation to which the Data Controller is subject or the transfer is made at the request of a regulator, police or other government agency (Article 12(1)(h));
- transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by legitimate interests of the Data Subject relating to the Data Subject's particular situation (Article 12(1)(i)); or
- transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that applies to a Data Controller (Article 12(1)(j)).

Authorities who may receive Personal Data in the context of a particular inquiry are not regarded as Recipients under the DPL or the DPRs (as per the definition of Recipient in the DPL).

SECURITY

Data Controllers must implement appropriate technical and organisational measures to protect Personal Data against wilful, negligent, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of Processing, in particular where Sensitive Personal Data is being Processed or where the Personal Data is being transferred out of the DIFC (Article 16(1)). When applying for a permit to Process Sensitive Personal Data, or Transfer Personal Data out of the DIFC, Data Controllers must include detail regarding the safeguards employed to ensure the security of such Sensitive Personal Data/Personal Data (respectively, Articles 2.1.1(i) and 5.1.1(i) of the DPR).

The measures implemented ought to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected (Article 16(2)).

BREACH NOTIFICATION

In the event of a breach (being an unauthorised intrusion, either physical, electronic or otherwise, to any Personal Data database, as defined by the DPL) Data Controllers (or Data Processors carrying out a Data Controller's function at the time of the breach), must inform the DPC of the incident as soon as reasonably practicable (Article 16(4)).

ENFORCEMENT

In the DIFC, the DPC oversees the enforcement of the DPL (Article 26).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The DPC needs to conduct all reasonable and necessary inspections and investigations before notifying a Data Controller that it has breached or is breaching the DPL or any regulations (Article 32). If the DPC is satisfied with the evidence of the breach, the DPC may issue a direction to the Data Controller requiring it to do either or both of the following:

- do or refrain from doing any act or thing within such time as may be specified in the direction (Article 33(1)); or
- refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction (Article 33(2)).

A Data Controller may ask the DPC to review the direction within fourteen days of receiving a direction and the DPC may receive further submissions and amend or discontinue the direction (Article 33(6)).

A Data Controller that fails to comply with a direction of the DPC may be subject to fines and liable for payment of compensation (Article 33(4)).

The DIFC Court may make any orders that it thinks just and appropriate in the circumstances, including remedies for damages, penalties or compensation (Article 37(2)).

ELECTRONIC MARKETING

As soon as possible upon beginning to collect Personal Data, the DPL requires Data Controllers to provide Data Subjects who they have collected Personal Data from, with, amongst other things, any further information to the extent necessary (having regard to the specific circumstances in which the Personal Data is collected). This includes information on whether the Personal Data will be used for direct marketing purposes (Article 13).

If the Personal Data has **not** been obtained from the Data Subject, the Data Controller or their representative must at the time of undertaking the Processing – or if it is envisaged that the Personal Data will be disclosed to a Third Party, no later than when the Personal Data is first Processed or disclosed – provide the Data Subject with, amongst other things, information regarding whether the Personal Data will be used for direct marketing purposes (Article 14).

Before Personal Data is disclosed for the first time to third parties or used on a Data Subject's behalf for the purposes of direct marketing, Data Subjects also have the right to be informed and to be expressly offered the right to object to such disclosures or uses (Article 18).

Additionally, the DPL requires a Data Controller to record various types of information regarding its Personal Data Processing operations (Article 19(4)). This must include an explanation of the purpose for the Personal Data Processing (Article 6.1.1(b) of the DPR). The DPR suggests that one of these purposes may be for advertising, marketing and public relations for the Data Controller itself or for others. (Article 6.2.1).

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

16. EGYPT

CONTRIBUTION DETAILS

John Matouk
Managing Partner
T +(202) 2795 4228/8179 (ext. 104)
john.matouk@dlamatoukbassiouny.com

Dr. Mohamed Ramadan
Senior Associate
T +(202) 2795 4288/8179 (ext. 113)
mohamed.ramadan@dlamatoukbassiouny.com

Mohamed Abdel Gawad
Associate
T +(202) 2795 4228/8179 (ext. 462)
mohamed.abdelgawad@dlamatoukbassiouny.com

Mohamed Fathy
Junior Associate
T +(202) 2795 4228/8179 (ext. 122)
mohamed.fathy@dlamatoukbassiouny.com

LAW

Egypt does not have a law which regulates protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt.

Constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data.

In addition, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Mentally Disordered Care Law no. 71/2009 has the same clause on confidentiality of the patient's data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The New Constitution has been promulgated in December 2012 and has replaced all the previous Constitutional Declarations issued by the Armed Forces Supreme Council and the President of the Arab Republic of Egypt.

The New Constitution has not defined data protection. However, it referred to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.

DEFINITION OF PERSONAL DATA

There is no definition of personal data or private life under Egyptian law or the New Constitution. However, Egyptian laws provide examples of the personal data that are protected such as the Labour Law. Article 77 of the Labour Law provides that the employees' files that must be kept by the employer (as mentioned below) includes the employee's personal data such as his name, job, professional skills when he joined the workplace, domicile, marital status, salary, starting date of his work, the holiday leave he takes, punishments imposed on him and the reports of his superiors on his work.

DEFINITION OF SENSITIVE PERSONAL DATA

There is no definition of sensitive personal data under Egyptian law.

NATIONAL DATA PROTECTION AUTHORITY

There is no national authority responsible for data protection in Egypt.

REGISTRATION

There is no requirement or facility to register data in a specific register.

DATA PROTECTION OFFICERS

There is no requirement in Egypt for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

According to the principles of the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary as an act or omission that violates an obligation imposed by the law or assumed caution and care of the average man.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Only data which is considered pertinent to the data subject's private life requires the consent of the data subject. The competent courts will determine whether specific data is considered pertinent to the private life of the data subject or not and whether the collection or processing of such data violates an obligation imposed by the law or assumed caution and care of the average man.

Collecting data about the employee is required by law (Article 77 of the Egyptian Labour Law) which provides that each employer must keep a file for each employee which includes their personal data. Only certain persons are authorised by the law to have access to such data.

TRANSFER

The same general principles applicable to data collection and processing mentioned above apply to the transfer of data; the data controller may not transfer data pertinent to the private life of the data subject except after obtaining the consent of the data subject, unless otherwise permitted by the law.

SECURITY

Other than client and account data in banks, personal data controllers are not required by law to take specific measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data. The data controllers will be held liable according to the average man standard if their acts or omissions cause the processing, loss, destruction or damage to such personal data and this in turn results in damage being caused to the data subject.

BREACH NOTIFICATION

There is no mandatory legal requirement in the Egyptian law to report data security breaches or losses to the authorities or to data subjects.

ENFORCEMENT

As a general rule, civil liability may be raised in connection with violations against the individuals' right to privacy. The prejudiced data subject should establish to the competent court the unlawful act, the damage occurred to them and the causation relationship between the unlawful act and the damage.

Civil liability for data privacy infringement has not been frequently claimed before Egyptian courts.

ELECTRONIC MARKETING

Egyptian law does not have any specific provisions which regulate Electronic Marketing.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Egyptian law does not have any specific provisions which regulate online privacy.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

17. FINLAND

CONTRIBUTION DETAILS

Hannes Snellman Attorneys Ltd
Eteläranta 8/P.O. Box 333, 00130 Helsinki, Finland
T +358 (9) 228 841
www.hannessnellman.com

Kaisa Fahllund
Partner
T +358 (9) 2288 4209
kaisa.fahllund@hannessnellman.com

Erkko Korhonen
Senior Associate
T +358 (9) 2288 4308
erkko.korhonen@hannessnellman.com

LAW

A member of the European Union, Finland implemented the EU Data Protection Directive 95/46/EC in June 1999 with the Personal Data Act 523/1999 ("**Act**").

DEFINITION OF PERSONAL DATA

Pursuant to the Act, "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 him or her or the members of his or her family or household.

DEFINITION OF SENSITIVE PERSONAL DATA

Pursuant to the Act, "sensitive personal data" means personal data that relates to or is intended to relate to (a) race or ethnic origin; (b) the social, political or religious affiliation or trade union membership of a person; (c) criminal act, punishment or other criminal sanction; (d) the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person; (e) the sexual preferences or sex life of a person; or (f) the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Ombudsman
P.O. Box 315
00181 Helsinki
Finland
Visiting address:
Albertinkatu 25 A, 3rd floor
T +358 29 56 66700
Website: www.tietosuoja.fi

REGISTRATION

There is no general obligation to register as a data controller under the Act. However, the data controllers shall make a notification to the Data Protection Ombudsman in certain situations. The notification shall be made if the processing of personal data is automated or the exemptions provided in the Act do not apply. Generally, the exemptions cover the majority of the general grounds for data processing. The duty of notification would concern e.g. the cases where the processing of personal data is outsourced or certain cases where personal data is transferred to outside the European Union or the European Economic Area or where the direct marketing is carried out.

However, pursuant to the Act, the data controller shall draw up a description of the personal data file, including the following information: (a) the name and address of the controller and, where necessary, those of the representative of the controller; (b) the purpose of processing the personal data; (c) a description of the group or groups of data subjects and the data or data groups relating to them; (d) the regular destinations of disclosed data and whether data is transferred to countries outside the European Union or the European Economic Area; and (e) a description of the principles in accordance to which the data file is secured.

The data controller shall keep the description of the file available to anyone apart from a few exceptions as set forth in the Act.

DATA PROTECTION OFFICERS

There is no specific requirement in the Act for organisations to appoint a data protection officer. However, entities processing personal data should appoint a contact person in the description of the personal data file.

COLLECTION AND PROCESSING

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

- the data subject has given his or her unambiguous consent for processing;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the data subject has given an assignment for processing, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
- processing is necessary, in an individual case, in order to protect the vital interests of the data subject;
- processing is based on the provisions of an Act, or it is necessary for compliance with a task or obligation to which the data controller is bound by virtue of an Act, or an order issued on the basis of an Act;
- there is a relevant connection between the data subject and the operations of the controller, because the data subject is a client or a member of, or in the service of, the controller or there is a comparable relationship between the two (connection requirement);
- the data relates to the clients or the employees of a group of companies or another comparable economic group, and they are processed within the said group;
- processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the data controller;
- the matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the data controller or a third party receiving the data; or
- the Data Protection Board has granted a permission for the processing of personal data in accordance with the Act.

There are separate requirements in the Act for the processing of sensitive personal data and the personal identity number. Further, in addition to these grounds, there are some specific purposes where the personal data may be processed such as historical, scientific or statistical purposes.

The purposes for the processing of personal data shall be defined in advance and personal data must not be processed in a manner incompatible with the defined purposes. Personal data shall only be processed to the extent necessary for the purposes of processing.

When collecting personal data, the data controller shall ensure that the data subject can have information on the data controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question.

TRANSFER

The data controllers may transfer personal data out of the European Union and the European Economic Area if any of the following conditions are met:

- the data subject has given his or her unambiguous consent to the transfer;
- the data subject has given an assignment for the transfer, or it is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the transfer is necessary in order to make or perform an agreement between the data controller and a third party and in the interest of the data subject;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is necessary or required by law in order to secure 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, from which data may be disclosed either generally of for special reasons as expressly prescribed by law;
- the data controller, by means of contractual terms or otherwise, gives adequate guarantees of the protection of the privacy and the rights of individuals, and the European Commission has not found, pursuant to Articles 3 and 26(3) of the Data Protection Directive, that the guarantees are inadequate; or
- the transfer is made by using standard contractual clauses as adopted by the European Commission in accordance with Article 26(4) of the Data Protection Directive.

Transfer of a data subject's personal data to non EU/European Economic Area countries is also allowed if the countries provide adequate levels of data protection as found by the European Commission, or if the level of data protection is sufficiently guaranteed by the data controller which are to be reviewed by the Data Protection Ombudsman.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the Finnish transfer provisions.

SECURITY

The controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised 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 shall be taken into account when carrying out the measures.

Anyone who operates on behalf of the data controller shall, before starting the processing of data, provide the data controller with appropriate commitments and other adequate guarantees of the data security.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the data subject or the data protection authorities (however, such obligations may be imposed on an entity elsewhere in legislation). However, the Data Protection Ombudsman or the Data Protection Board may instruct the data controller to take necessary actions and these may include informing the data subjects on the breach.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

The Data Protection Ombudsman and the Data Protection Board are responsible for the enforcement of the Act.

The Data Protection Ombudsman provides direction and guidance on the processing of personal data and supervises the data processing. It also issues directions, advice and guidelines in order to cease and prevent unlawful conduct. Where necessary, the Data Protection Ombudsman shall refer the matter to be dealt with by the Data Protection Board, or report it for prosecution.

The Data Protection Board may, upon request made by the Data Protection Ombudsman (a) prohibit processing of personal data which is contrary to the Act or the rules and regulations issued on the basis of the Act; (b) compel the person concerned to remedy an instance of unlawful conduct or neglect; (c) order that the operations concerning processing of personal data be ceased if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his or her interests or rights, provided that the personal data file is not set up under a statutory scheme; and (d) revoke a permission to process personal data which it has granted and where the prerequisites for processing are no longer fulfilled or the controller has failed to comply with the permission or the rules attached to it.

Failure to comply with the Act may result in criminal liability under the Finnish Penal Code (38/1889) or the Act and be punished with fines or imprisonment in the maximum of one year.

ELECTRONIC MARKETING

Direct marketing by electronic means is regulated by the Finnish Act on the Protection of Privacy in Electronic Communications 2004/516 (the "**ECA**"), which came into force on 1 September 2004. The Data Protection Ombudsman shall have the power to supervise the compliance with the provisions on direct marketing.

Pursuant to the ECA, direct marketing may only be directed to natural persons by means of automated calling systems, facsimile machines, or e-mail, text, voice, sound or image messages if they have given their prior consent. Direct marketing other than by electronic means is allowed if a natural person has not specifically prohibited it. However, where a service provider has obtained contact information of a natural person in the context of the sale of a product or service, that service provider may generally use this information for direct marketing of his/her own products of the same product group and of other similar products or services, unless prohibited by the natural person in question.

Direct marketing to legal persons is allowed if the recipient has not specifically prohibited it. Both natural persons and legal persons must be allowed to prohibit all direct marketing referred to above easily and at no charge. Telecommunications operators and corporate or association subscribers are entitled, at a user's request, to prevent the reception of such direct marketing.

Under the ECA, there are additional requirements concerning the identification of direct marketing. Firstly, the recipient of an e-mail, text, voice, sound or image message sent for the purpose of direct marketing must be able to recognize such a message as marketing clearly and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

unambiguously. Secondly, it is prohibited to send such message intended for marketing that either conceals the identity of the sender, is without a valid address or solicits recipients to visit websites that contravene the provisions of the Consumer Protection Act.

Moreover, as there is likely to be processing of personal data involved in the electronic marketing, the provisions of the Personal Data Act (the "**Act**") will be applicable. Generally, a data subject shall have a right to prohibit the controller from processing his/her personal data for direct advertising and other direct marketing. If such processing has not been prohibited by the data subject, personal data may be collected into a personal data file kept for the purposes of direct marketing, if other requirements of the Act are met.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Online privacy matters such as cookies and location data are regulated by the Finnish Act on the Protection of Privacy in Electronic Communications 2004/516 (the "**ECA**").

Cookies – The service provider may save cookies or other data in the user's terminal device, if the user has given his/her consent thereto. The term "consent" is interpreted in the preliminary works of the law so that it may be given via browser or other application settings. Moreover, ECA requires that the service provider gives the user comprehensible and complete information on the purposes of saving or using such data. The saving and use of data is allowed only to the extent required for the service, and it may not limit the protection or privacy any more than is necessary.

However, the above mentioned provisions regarding saving and using of cookies do not apply to any processing of data which is intended solely for the purposes of enabling the transmission of messages or which is necessary for the service provider to be able to provide a service that has been specifically requested by the subscriber or user.

Location Data – Pursuant to the ECA, all messages, identification data and location data are confidential unless otherwise provided. Location data may be processed by telecom operators, value added service providers or corporate or association subscribers for the purpose of providing and using value added services. Such processing is allowed only to the extent required for the purpose of the processing, and it shall not limit the protection of privacy any more than is necessary.

Before beginning the processing of location data, the value added service provider or the corporate or association subscriber shall request service-specific consent from the party to be located, unless such consent is implied from the context or otherwise provided by law. It shall be ensured that the party to be located has both easy and continuous access to information on the location of the data processed and at no separate charge to cancel the consent.

A telecommunications operator shall have the right to process location data if the subscriber has not forbidden it. Before disclosing location data to a value added service provider or corporate or association subscriber, the telecommunications operator shall take appropriate steps to ensure that the provision of such a value added service is based on the consent from the party to be located as stated above.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

18. FRANCE

CONTRIBUTION DETAILS

Carol A.F. Umhoefer
Partner
T +331 4015 2400
carol.umhoefer@dlapiper.com

LAW

Law No. 78 17 of 6 January 1978 on "Information Technology, Data Files and Civil Liberty" ("**Law**") is the principal law regulating data protection in France.

The EU Data Protection Directive 95/46/EC was implemented via Law No. 2004 8021 of 6 August 2004 which amended the Law.

Enforcement of the Law is principally through the "*Commission Nationale Informatique et Libertés*" (**"CNIL"**).

DEFINITION OF PERSONAL DATA

Any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him or her.

DEFINITION OF SENSITIVE PERSONAL DATA

Personal data that reveals directly or indirectly, racial and ethnic origins, political, philosophical, religious opinions or trade union affiliation of persons, or that concern their health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale de l'Informatique et des Libertés (CNIL)
8, rue Vivienne
CS 30223
75083 Paris Cedex 02
T 01 53 73 22 22
F 01 53 73 22 00
http://www.cnil.fr/english/

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The CNIL is responsible for ensuring that information technology remains at the service of citizens, and does not jeopardize human identity or breach human rights, privacy or individual or public liberties.

REGISTRATION

Except for certain data processing that is subject to exemption, authorization, ministerial order or decree issued by the Supreme Administrative Court ("**Conseil d'Etat**"), the processing of personal data requires a prior declaration to the CNIL.

The prior declaration to the CNIL shall specify, amongst other things:

- the purpose(s) of the processing;
- the identity and the address of the data controller (i.e. the natural or legal person who determines the purpose and the means of the personal data processing and implements such decisions itself or appoints a data processor to implement them);
- the possible interconnections between databases;
- the types of personal data processed and the categories of persons concerned by the processing;
- the recipients of the processed data;
- the time period for which the data will be kept;
- the department or person(s) in charge of implementing the data processing;
- the recipients or categories of recipients of the personal data;
- the measures taken in order to ensure the security of the processing; and
- the existence of a data transfer to a country outside of the EU regarded by the CNIL as not providing an adequate level of protection.

The CNIL may also exempt certain processes from prior declaration, in view of their purposes, addressees, the nature of the processed data, the length of their conservation or the concerned persons. Other processes may require only a simplified prior declaration.

DATA PROTECTION OFFICERS

There is no legal requirement for organisations to appoint a data protection officer (known as a **Correspondant Informatique et Libertés or CIL** in France).

However, an organisation is exempt from making prior declarations to the CNIL if the organisation has appointed a data protection officer ("**DPO**").

The appointment of a DPO does not exempt an organisation from requesting prior authorisation, where necessary (e.g. transfer of data to a country that does not provide an adequate level of protection to personal data).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The DPO is in charge of verifying the compliance of data processing with the Law. The DPO communicates, to any person who requests, information on the processing such as its purposes, interconnections, the types of data and the categories of concerned persons, the length of data conservation and the services in charge of implementing the processing.

COLLECTION AND PROCESSING

Any personal data must be processed in a manner consistent with the following general principles:

- all personal data is processed fairly and lawfully;
- all personal data is collected for specific, explicit and legitimate purposes and are subsequently processed in accordance with these purposes;
- all personal data collected is adequate, relevant, and non excessive in view of the purposes for which they are collected; and
- all personal data is accurate, comprehensive and, when necessary, kept up to date.

The processing of personal data shall have received the individual's consent or shall fulfil one of the following conditions:

- processing is required by law;
- the purpose of the processing is to protect the individual's life;
- the purpose of the processing is to carry out a public service;
- processing relates to the performance of a contract to which the concerned individual is a party; or
- processing relates to the realisation of the legitimate interest of the data controller or of the data recipient, subject to the interest and fundamental rights and liberties of the concerned individual.

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

Whichever of the above conditions is relied upon, the person from whom the personal data is collected must be informed of:

- the identity of the data controller and, as the case may be, the data processor;
- the purposes of the data processing;
- the recipients or categories of recipients of the data;
- the right to object, for a legitimate purpose, to the collection of such data, a right to access the collected data and a right to have the processed data rectified, completed, blocked or deleted; and
- where data is to be transferred outside the EU, and specific details on where and why the data is newly transferred.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

Transfer of a data subject's personal data to a non EU/European Economic Area country is allowed if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties. The sufficient nature of the protection is assessed taking into account national laws, applicable security measures, specific characteristics of the processing, such as its purpose and duration, as well as the nature, origin and destination of the processed data.

For data transfers to the United States, companies that adhere to the US/EU Safe Harbor principles are deemed to offer adequate protection.

Data controllers may transfer personal data out of the European Economic Area to countries that are not deemed to offer adequate protection if the transfer is necessary:

- for the protection of the individual's life;
- for the protection of the public interest;
- to comply with obligations allowing the acknowledgement, the exercise or the defence of a legal right;
- for consultation of a public register intended for the public's information;
- for the performance of a contract between the data controller and the individual, or pre contractual measures undertaken at the individual's request;
- for the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party.

The CNIL may allow transfers if the above conditions are not fulfilled provided there is an adequate level of protection by reason of contractual provisions e.g. by standard contractual clauses (Model Clauses) approved by the European Commission, or internal rules (Binding Corporate Rules) applicable to data exporter and data importer.

SECURITY

The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, amongst other things, prevent alteration, corruption or access by unauthorised third parties.

A data processor may only process personal data on behalf and upon instruction given by the data controller. The data processor must provide sufficient guarantees in terms of security and confidentiality, but even if this is the case, the data controller remains liable for compliance with these obligations.

BREACH NOTIFICATION

The Law does not set out any obligation to notify the CNIL or the data subject in the event of a data security breach.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

The CNIL has the power to proceed with verifications of any data processing, and, as the case may be, to request a copy of every document that it considers useful in view of its mission. The CNIL also has the power to pronounce different sanctions that vary in accordance with the severity of the violation committed by the data controller:

- warnings and notices to comply with the obligations defined in the Law; or
- if the data controller does not comply with the notice, the CNIL has the power to order a financial sanction up to EUR 150,000 for the first violation, and in the case of a second violation in the following 5 years, up to EUR 300,000 or 5% of the company's turnover (limited to EUR 300,000), and/or to order that the company immediately cease the data processing.

In accordance with Articles 226 16 to 226 24 of the French Criminal Code, various violations of the Law may constitute a misdemeanour. For example, the violation, even by negligence, of the prior declaration requirements (see Registration above) is punishable by up to 5 years' imprisonment, and/or a fine of up to EUR 300,000 (for natural persons), or a fine up to EUR 1.5M and/or other sanctions (for legal persons).

ELECTRONIC MARKETING

The Act does not contain explicit provisions with respect to electronic marketing. However the CNIL has issued guidelines on the basis of French consumer law and electronic communications law.

The CNIL distinguishes between B2B and B2C relationships.

In any event, all electronic marketing messages must specify the name of the advertiser and allow the recipient to object to the reception of similar messages in the future.

Electronic marketing to consumers (B2C):

Electronic marketing activities are authorised provided that the recipient has given consent at the time of collection of his/her email address.

This principle does not apply when:

- the concerned individual is already a customer of the company and if the marketing messages sent pertain to products or services similar to those already provided by the company.
- the marketing messages are not commercial in nature.

In any event the concerned individual must be informed at the time of collection of his/her email address (i) that it will be used for electronic marketing activities (ii) that he/she may object to such use.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Electronic marketing to professionals (B2B):

Electronic marketing activities are authorised provided that the recipient has been informed at the time of collection of his/her email address (i) that it will be used for electronic marketing activities (ii) that he/she may object to such use.

The message sent must relate to the concerned individual's professional activity.

Please note that email addresses such as contact@companyname.fr are not subject to prior consent and right to object.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookies – The EU Cookie Directive has been implemented in the Law. It states that any subscriber or user of electronic communications services must be fully and clearly informed by the data controller or its representative of (i) the purpose of any cookie (i.e. any means of accessing or storing information on the subscriber's/user's computer), and (ii) the means of refusing cookies, unless the subscriber/user has already been so informed. Cookies are lawfully deployed only if the subscriber/user has expressed consent after having received such information.

However, the foregoing provisions do not apply (i) to cookies the sole purpose of which is to allow or facilitate electronic communication by a user, or (ii) if the cookie is strictly necessary to provide on line communication services specifically requested by the user.

In November 2011 and again in April 2012, the CNIL issued guidance for cookies.

The CNIL considers that certain cookies are not covered by the Law (e.g. cookies used to constitute a "basket" on a e-commerce platform, session ID cookies etc).

Regarding consent, the CNIL has specified that consent must be (i) freely given (i.e. in circumstances where the user has a choice to refuse consent), (ii) specific (i.e. relate to a specific cookie associated with a clearly defined purpose), and (iii) informed (i.e. the user must be given information beforehand, specifying the cookie's purpose as well as the possibility to revoke consent). Valid consent can be expressed via browser settings if the user can choose the cookies he/she accepts and for which purpose. However, according to the CNIL, commonly used browsers do not offer compliant settings.

The CNIL regards the following consent collection mechanisms as compliant:

- a banner at the top of a webpage;
- a consent request zone overprinting on the site's homepage; and
- boxes to tick when registering for an online service.

The CNIL considers that the website owner is liable for allowing a third party to install a cookie on the user's computer.

The April 2012 guidance also reaffirms that these rules apply to all cookies whether containing personal data or not.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The April 2012 guidance also reminds operators that non-compliance with French law can trigger financial penalties (see enforcement section).

Location and Traffic Data – The Postal and Electronic Communications Code deals with the collection and processing of location and traffic data by electronic communication service providers ("**CSPs**").

All traffic data held by a CSP must be erased or anonymised. However, traffic data may be retained e.g.:

- for the purpose of finding, observing and prosecuting criminal offences;
- for the purpose of billing and payment of electronic communications services; or
- for the CSP's marketing of its own communication services, provided the user has given consent thereto.

Subject to exceptions (observing and prosecuting criminal offences; billing and payment of electronic communications services), location data may be used in very limited circumstances, e.g.:

- during the communication, for the proper routing of such communication; or
- where the subscriber has given informed consent, in which case the location data may be processed and stored after the communication has ended.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

19. GERMANY

CONTRIBUTION DETAILS

Thomas Jansen
Partner
T +49 89 2323 72 110
thomas.jansen@dlapiper.com

Britta Hinzpeter
Senior Associate
T +49 89 2323 72 112
britta.hinzpeter@dlapiper.com

Patrick Schwarzbart
Senior Associate
T +49 89 2323 72 113
patrick.schwarzbart@dlapiper.com

LAW

The main legal source of data protection in Germany is the Federal Data Protection Act (Bundesdatenschutzgesetz in German) ("**BDSG**") which implements the European data protection directive 95/46/EC.

Additionally, each German state has a data protection law of its own. In principle, the data protection acts of the individual states intend to protect personal data from processing and use by public authorities of the states whereas the BDSG intends to protect personal data from processing and use by federal public authorities and private bodies. Enforcement is through the data protection authorities of the German states. The competence of the respective state authority depends on the place of business of the data controller.

DEFINITION OF PERSONAL DATA

The BDSG defines personal data as any information concerning the personal or material circumstances of an identified or identifiable natural person ("**data subject**").

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive or rather special categories of personal data under the BDSG are any information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Each individual German state has a Data Protection Authority which is responsible for the enforcement of data protection laws and competent for data controllers established in the relevant state.

REGISTRATION

Unlike most European data protection regimes, German data protection law does not require a registration of automated data processing. In addition, even though the BDSG provides for a notification, such notification is the exception rather than the rule.

This follows from the fact that the notification requirement is waived if the data controller has appointed a data protection officer ("**DPO**"), which is mandatory for all companies of a certain size (the obligation applies if more than nine persons are regularly involved in the automated processing of personal data). Automated data processing operations with respect to sensitive data are subject to prior checking by the data controller's internal DPO.

DATA PROTECTION OFFICERS

Data controllers that deploy more than nine persons with the automated processing of personal data are obliged to appoint a DPO. Such a DPO may either be an employee or an external consultant that has sufficient knowledge in the field of data protection.

The DPO shall in particular monitor the proper use of data processing programs and take suitable steps to familiarise the persons employed in the processing of personal data with the provisions of data protection.

As far as sensitive personal data is concerned, such personal data is subject to examination prior to the beginning of processing (prior checking) by the appointed DPO unless the data subject has consented. In case of doubt, the DPO shall liaise with the competent authorities.

COLLECTION AND PROCESSING

The collection, processing and use of personal data is only admissible if explicitly permitted by the BDSG or any other legal provision or if the data subject has explicitly consented in advance.

In practice, Section 28 BDSG is the most applicable statutory provision permitting collection, processing and use of personal data. For example, Section 28 para. 1 no. 1–3 BDSG provide that the collection, processing or use of personal data as a means of fulfilling one's own business purposes shall be admissible if it is:

- necessary to create, perform or terminate a legal obligation or quasi legal obligation with the data subject;
- necessary to safeguard legitimate interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the personal data is generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding interest.

Sensitive personal data may only be processed if:

- it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent;
- the data involved has manifestly been made public, by the data subject;
- it is necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of collection, processing or use; or
- it is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, processing and use and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort.

Processing of employee data for employment related purposes is subject to a separate provision (Sec. 32 BDSG) according to which the collection, processing and use of employee data is only permitted regarding decisions on the establishment, implementation and termination of the employment contract.

Whichever of the above conditions is relied upon, upon the first collection of personal data without the data subject's knowledge, the data controller must provide the data subject with "fair processing information". This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

With respect to the transfer of personal data to third parties it needs to be differentiated between a transfer within the European Economic Area **("EEA")** and a transfer to any other country outside the EEA:

- Due to the harmonisation of data protection law by European law, a transfer of personal data to third parties within the EEA is treated as if it took place within the territory of Germany, ie it is admissible if explicitly permitted by the BDSG or any other legal provision or if the data subject has explicitly consented in advance.
- The transfer of personal data to a country outside the EEA (**"cross border"**) is admissible provided the following conditions are fulfilled:
  - regardless of the fact that the personal data is transferred cross border, a legal basis for the transfer as such is required, i.e. in the absence of consent, it needs to be explicitly permitted by the BDSG or any other legal provision; and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the data recipient needs to ensure an adequate level of data protection. The European – Commission considers data recipients in Andorra, Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Faeroe Islands Israel and New Zealand as providing such an adequate level (as of 19 December 2012). In case the data recipient is seated in the US, it should comply with the US Department of Commerce's Safe Harbour Privacy Principles. In addition, adequate safeguards with respect to the protection of personal data can be achieved by entering into binding corporate rules (only applicable if the data recipient is a group company) or by entering into a data protection agreement based on the EU model clauses of the European Commission). Please note that a data transfer agreement based on the EU model clauses must be strictly in compliance with the wording of the model clauses provided by the EU Commission.

- Whether there is a notification requirement, depends on the legal basis for the cross-border transfer. While a transfer based on binding corporate rules always requires involvement of the authorities, a transfer based on Safe Harbour principles or EU model clauses does not. Such transfer is handled differently by the responsible authorities. However, most authorities do not require a notification.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm which might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data.

BREACH NOTIFICATION

A breach notification duty has recently been implemented into the BDSG. According to Sec. 42a BDSG the notification duty applies if:

- sensitive personal data; personal data subject to professional secrecy, personal data related to criminal and/or administrative offences, personal data concerning bank or credit card accounts, certain telecommunications and online data is abused or lost and an authorised third party acquires knowledge; and
- in case of telecommunications and online data, there is a serious threat of interference with interests of concerned individuals.

Data controllers are obliged to inform supervisory authorities and the concerned individuals.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

Violation of German data protection laws are subject to pecuniary fines up to EUR 300,000 per violation (administrative offence). In the case of wilful behaviour or if conducted in exchange for a financial benefit (criminal offence), by imprisonment of up to 2 years or a fine depending on how severe the violation is. Authorities may also skim profits generated by data protection breaches.

In the past, German data protection authorities were rather reluctant concerning the enforcement of data protection law, ie very few official prosecution procedures were opened and imposed fines were rather low. However, this has recently changed and we note a tendency to a stricter enforcement. This particularly relates to several data protection scandals involving loss and disclosure or misuse of personal data in the recent years.

Further, reputation damages are usually quite severe if data protection breaches become public. Civil liabilities as well as injunctive reliefs and skimming of profits are likely under the Unfair Competition Act.

ELECTRONIC MARKETING

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the "same service/product" exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided:

- the user has been informed of the right to opt-out prior to the first marketing email;
- the user did not opt-out; and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communication sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Traffic data – Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent:

- the number or other identification of the lines in question or of the terminal;
- authorisation codes, additionally the card number when customer cards are used;
- location data when mobile handsets are used;
- the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted;
- the telecommunications service used by the user; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted.

Any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or in case the user has requested a connection overview.

Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection.

Location Data – Location Data qualifies as personal data. This data may only be processed as required for the provision of requested services and is subject to prior information of the user. For all other purposes, the user's informed consent must be obtained. According to Section 4a BDSG, 13 German Telemdia Act ("**TMG**") this means that:

- the user's consent must be intentional, informed and clear. For this purpose the user must be informed on the type, the scope, the location and the purpose of data collection, processing and use including any forwarding of data to third parties;
- the user's consent must be recorded properly ;
- the user must be able to access the content of his consent declaration any time. It is sufficient that such information are provided upon the users' request; and
- the user's consent must be revocable at all times with effect for the future.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Users must always be informed on the use of cookies in a privacy notice. Cookies may generally be used if they are required in order to perform the services requested by the user. Otherwise, users must be provided with an opt-out mechanism. For this purpose, information on the use of cookies together with a link on how to adjust browser settings in order to prevent future use is sufficient.

Germany has not yet implemented the e-privacy directive. It is currently unclear when this will happen. It therefore remains to be seen whether it would also be sufficient to link the information about processing of personal data and technical measures to the browser settings or whether an active opt-in, e.g. by clicking on a pop-up screen will be required in the future.

Different rules apply in the case of tracking technologies which collect and store a user's IP address. Since IP addresses qualify as personal data, their processing for tracking and marketing services requires active opt-in consent.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

20. GIBRALTAR

CONTRIBUTION DETAILS

Hassans
www.gibraltarlaw.com

Michael Nahon
Senior Associate
T (+350) 200 79000
michael.nahon@hassans.gi

LAW

A territory within the European Union (by virtue of the accession of the United Kingdom on 1 January 1973) Gibraltar implemented the EU data Protection directive 95/46 EC in 2006 with the Data Protection Act 2004 ("**Act**"). Enforcement is through the offices of the Data Protection Commissioner ("**DPC**").

DEFINITION OF PERSONAL DATA

Any information relating to a Data Subject; and a Data Subject means a natural person who is the subject of Personal Data.

DEFINITION OF SENSITIVE PERSONAL DATA

Information about racial or ethnic origin, religious or philosophical beliefs, trade union membership, health or sex life. The definition includes data regarding the commission or alleged commission of any offence and information on any proceedings for offences or alleged offences, the disposal of such proceedings and any sentence given.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commissioner

Gibraltar Regulatory Authority
Suite 603 Europort
Gibraltar
T 200 74636
F 200 72166
info@gra.gi

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

Data controllers who process personal data must notify the Data Protection Commissioner by registering with the Gibraltar Regulatory Authority ("**GRA**") so that their processing of personal data may be registered and made public in the Data Protection Register, unless an exemption applies. Once registered any changes to the processing of personal data will require the Data Protection Register to be updated.

The notification must contain the following information:

- name and address of data controller and any representative;
- description of the personal data being processed and the categories to which they relate;
- description of the purpose of the processing;
- description of the recipients or categories of recipient to who data will be sent;
- names of any countries outside the EEA to which data is to be transferred to;
- an adequate description of the security measures taken that is sufficient to allow a preliminary assessment of those measures; and
- other information reasonably required by the DPC.

DATA PROTECTION OFFICERS

There is no requirement in Gibraltar for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

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

- the data subject has unambiguously given his consent;
- the processing is necessary for the performance of a contract to which the data subject is a party, or for actions to be carried out at the request of the data subject prior to entering into a contract;
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject;
- the processing is necessary to prevent:
  - injury or other damage to the health of the data subject;
  - serious loss or damage to his property;
  - to protect his vital interests where seeking consent is likely to damage those interests;
- the processing is necessary for a public purpose, namely:
  - for the administration of justice;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- for the performance of a statutory function;
- for the performance of a function of Government or of a Government Minister;
- the processing is necessary for the performance of a public function carried out in the public interest; and
- the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplies, except where the rights of the data subject under the European Convention of Human Rights and the Gibraltar Constitution prevail.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.

TRANSFER

Data controllers may transfer personal data out of the EEA if any of the following conditions are met:

- the country to which the data is being transferred ensures an adequate level of protection by reference to statutory parameters;
- the data subject consents to the transfer;
- the transfer is necessary:
  - to perform a contract between the data subject and the data controller;
  - to take steps at the request of the data subject in order to enter into a contract with the data controller;
  - for the agreement or performance of a contract between a third party;
  - and the data controller at the request of the data subject;
  - the transfer of data is required pursuant to an international obligation of Gibraltar;
  - the transfer is necessary due to a substantial public interest;
  - the transfer is necessary to obtain legal advice either in respect of proceedings or to establish or defend a legal right;
  - the transfer is necessary to protect the vital interests of the data subject; and
  - the transfer is made as part of personal data stored on a public register.

If none of these conditions are met, data outside of the EEA may still be transferred if:

- it is to a country approved by the EU commission as safe;
- it is to a US organisation falling within the Safe Harbour provisions; or
- on terms incorporating the Model Clauses or approved Corporate Binding Rules.

Alternatively the data controller can apply to the DPC for specific approval on a case by case basis.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Data controllers must take appropriate technical and organisational measures against accidental or unlawful destruction, loss or alteration of data, or against unauthorised disclosure or access to the information, and generally against all other unlawful forms of processing.

BREACH NOTIFICATION

There is currently no mandatory requirement in the Act to report data security breaches or losses to the DPC or to data subjects. A mandatory requirement will be introduced with the transposition into Gibraltar law of the Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications) introduced by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

ENFORCEMENT

In Gibraltar, the DPC is responsible for the enforcement of the Act. If he becomes aware that the data controller is in breach of the Act, he can initiate proceedings against the data controller.

The ultimate sanction on conviction for an offence is a fine of GBP 2,000 (in the case of summary conviction in the magistrate's court) or GBP 5,000 (in the case of indictment in the Supreme Court).

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be "personal data" for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (e.g. a right to "opt out") for direct marketing purposes.

The Communications (PD&P) Regulations 2006 ('**the Regulations**') prohibit the use of automated calling systems without the consent of the recipient and unsolicited emails can only be sent without consent if:

- The contact details have been provided in the course of a sale or negotiations;
- The marketing relates to a similar product or services; and
- The recipient was given a means of refusing the use of their contact details for marketing when they were collected.

Direct marketing emails must not disguise or conceal the identity of the sender in contravention of the E-Commerce Act. SMS marketing is also likely to be included within the prohibition on email marketing.

The restrictions on marketing by email only apply in relation to individuals and not where email marketing is sent to corporations.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The Regulations deal with the collection of location and traffic data by public electronic communications providers ("**CPs**") and the use of cookies (and similar technologies).

Traffic Data – Traffic Data held by a CP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service; and
- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CP for:

- The management of billing or traffic;
- Dealing with customer enquiries;
- The prevention of fraud;
- The marketing of electronic communications services; or
- The provision of a value added service.

Location Data – Location Data may only be processed for the provision of value added services with consent and where the identity of the user is anonymised. CPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Cookie Compliance – The use and storage of cookies and similar technologies requires: a) clear and comprehensive information; and b) consent of the website user. Usual data protection principals of the Act also apply. Consent is not required for cookies that are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network or where this is strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the Regulations is dealt with by the DPC and if found guilty a fine and or imprisonment may be imposed. However an individual may also bring an action for damages in the Supreme Court.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

21. GREECE

CONTRIBUTION DETAILS

Kyriakides Georgopoulos & Daniolos Issaias Law Firm
www.kgdi.gr

Effie Mitsopoulou
Partner
T +30 210 817 1540
e.mitsopoulou@kgdi.gr

LAW

Greece implemented the EU Data Protection Directive 95/46/EC in October 1997 with Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, as amended ("**Law**"). Such law is currently in force as amended by Laws 3471/2006 3783/2009. 3947/2011, 4024/2011 and 4070/2012.

Enforcement is through the Data Protection Authority ("**DPA**").

DEFINITION OF PERSONAL DATA

"Personal data" shall mean any information relating to the data subject. Personal data is not considered to be the consolidated data of a statistical nature where data subjects may no longer be identified.

DEFINITION OF SENSITIVE PERSONAL DATA

"Sensitive data" shall mean the data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, social welfare and sex life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Authority
1-3 Kifissias Avenue
T 2106475600
F 2106475628
contact@dpa.gr

The DPA is responsible for overseeing the Data Protection Law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

The data controller must notify the DPA in writing about the establishment and operation of a file or the commencement of data processing. In the course of the aforementioned notification, the data controller must necessarily declare the following:

- His/her name, trade name or distinctive title, as well as his/her address;
- The address where the file or the main hardware supporting the data processing is established;
- The description of the purpose of the processing of personal data included or about to be included in the file;
- The category of personal data that is being processed or about to be processed or included or about to be included in the file;
- The time period during which s/he intends to carry out data processing or preserve the file;
- The recipients or the categories of recipients to whom such personal data is or may be communicated;
- Any transfer and the purpose of such transfer of personal data to third countries; and
- The basic characteristics of the system and the safety measures taken for the protection of the file or data processing.

The above data is then registered with the Files and Data Processing Register kept by the DPA. Any modification of the above data must be communicated in writing and without any undue delay by the data controller to the DPA.

DATA PROTECTION OFFICERS

There is no requirement in Greece for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

Collection and processing of personal data is permitted only when the data subject has given his/her consent. Exceptionally, data may be processed even without such consent, but only if:

- processing is necessary for the execution of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for the compliance with a legal obligation to which the data controller is subject;
- processing is necessary in order to protect the vital interests of the data subject, if s/he is physically or legally incapable of giving his/her consent;
- processing is necessary for the performance of a task carried out in the public interest or a project carried out in the exercise of public function by a public authority or assigned by it to the data controller or a third party to whom such data are communicated; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- processing is absolutely necessary for the purposes of a legitimate interest pursued by the data controller or a third party or third parties to whom the data is communicated and on condition that such a legitimate interest evidently prevails over the rights and interests of the persons to whom the data refer and that their fundamental freedoms are not affected.

Processing sensitive personal data:

The collection and processing of sensitive data is prohibited. Exceptionally, the collection and processing of sensitive data, as well as the establishment and operation of the relevant file, is permitted by the DPA, when one or more of the following conditions occur:

- the data subject has given his/her written consent, unless such consent has been extracted in a manner contrary to the law or bonos mores or if law provides that any consent given may not lift the relevant prohibition;
- processing is necessary to protect the vital interests of the data subject or the interests provided for by the law of a third party, if s/he is physically or legally incapable of giving his/her consent;
- processing relates to data made public by the data subject or is necessary for the recognition, exercise or defence of rights in a court of justice or before a disciplinary body;
- processing relates to health matters and is carried out by a health professional subject to the obligation of professional secrecy or relevant codes of conduct, provided that such processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services;
- processing is carried out by a Public Authority and is necessary for the purposes of a) national security, b) criminal or correctional policy and pertains to the detection of offences, criminal convictions or security measures, c) protection of public health or d) the exercise of public control on fiscal or social services;
- processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken; or
- processing concerns data pertaining to public figures, provided that such data are in connection with the holding of public office or the management of third parties' interests, and is carried out solely for journalistic purposes. The DPA may grant a permit only if such processing is absolutely necessary in order to ensure the right to information on matters of public interest, as well as within the framework of literary expression and provided that the right to protection of private and family life is not violated in any way whatsoever.

The DPA grants a permit for the collection and processing of sensitive data, as well as a permit for the establishment and operation of the relevant file, upon request of the data controller. The permit is issued for a specific period of time, depending on the purpose of the data processing. It may be renewed upon request of the data controller.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The permit must necessarily contain the following:

- The full name or trade name or distinctive title, as well as the address, of the data controller and his/her representative, if any;
- The address of the place where the file is established;
- The categories of personal data which are allowed to be included in the file;
- The time period for which the permit is granted;
- The terms and conditions, if any, imposed by the DPA for the establishment and operation of the file; and
- The obligation to disclose the recipient or recipients as soon as they are identified.

A copy of the permit is registered with the Permits Register kept by the DPA. Any change in the above data must be communicated without undue delay to the DPA. Any change other than a change of address of the data controller or his/her representative must entail the issuance of a new permit, provided that the terms and conditions stipulated by law are fulfilled.

TRANSFER

The transfer of personal data is permitted:

- For member states of the European Union;
- For a non member of the European Union following a permit granted by the DPA if it deems that the country in question guarantees an adequate level of protection. For this purpose it shall particularly take into account the nature of the data, the purpose and the duration of the processing, the relevant general and particular rules of law, the codes of conduct, the security measures for the protection of personal data, as well as the protection level in the countries of origin, transit and final destination of the data. A permit by the DPA is not required if the European Commission has decided, on the basis of the process of article 31, paragraph 2 of Directive 95/46/EC of the Parliament and the Council of 24 October 1995, that the country in question guarantees an adequate level of protection, in the sense of article 25 of the aforementioned Directive;

The transfer of personal data to a non member state of the European Union which does not ensure an adequate level of protection is exceptionally allowed only following a permit granted by the DPA, provided that one or more of the following conditions occur:

- the data subject has consented to such transfer, unless such consent has been extracted in a manner contrary to the law or bonos mores; and
- the transfer is necessary:
  - in order to protect the vital interests of the data subject, provided s/he is physically or legally incapable of giving his/her consent;
  - for the conclusion and performance of a contract between the data subject and the data controller or between the data controller and a third party in the interest of the data subject, if he/she is incapable of giving his/her consent; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

  - for the implementation of pre contractual measures taken in response to the data subject's request;
- the transfer is necessary in order to address an exceptional need and safeguard a superior public interest, especially for the performance of a co operation agreement with the public authorities of the other country, provided that the data controller provides adequate safeguards with respect to the protection of privacy and fundamental liberties and the exercise of the corresponding rights;
- the transfer is necessary for the establishment, exercise or defence of a right in court;
- the transfer is made from a public register which by law is intended to provide information to the public and which is accessible by the public or by any person who can demonstrate legitimate interest, provided that the conditions set out by law for access to such register are in each particular case fulfilled; or
- the data controller shall provide adequate safeguards with respect to the protection of the data subjects' personal data and the exercise of their rights, when the safeguards arise from conventional clauses which are in accordance with the regulations of the Law. A permit is not required; in case of the Standard Contractual Clauses approved by the European Commission; in cases where the data importer has been registered with the Safe Harbor Framework; and finally in cases where the Binding Corporate Rules have been executed.

SECURITY

The processing of personal data must be confidential. It must be carried out solely and exclusively by persons acting under the authority of the data controller or the processor and upon his/her instructions.

In order to carry out data processing the data controller must choose persons with corresponding professional qualifications providing sufficient guarantees in respect of technical expertise and personal integrity to ensure such confidentiality.

The data controller must implement appropriate organisational and technical measures to secure data and protect it against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing.

If the data processing is carried out on behalf of the data controller, by a person not dependent upon him, the relevant assignment must necessarily be in writing. Such assignment must necessarily provide that the processor carries out such data processing only on instructions from the data controller and that all other confidentiality obligations must *mutatis mutandis* be borne by him.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

There is no mandatory requirement in the Law to report data security breaches or losses to the DPA or to data subjects.

ENFORCEMENT

The DPA may impose on the data controllers or on their representatives, if any, the following administrative sanctions for breach of their duties arising from the Law as well as from any other regulation on the protection of individuals from the processing of personal data:

- a warning with an order for the violation to cease within a specified time limit;
- a fine amounting between EUR 880 and EUR 147,000;
- a temporary revocation of the permit;
- a definitive revocation of the permit; or
- the destruction of the file or a ban of the processing and the destruction, return or locking of the relevant data.

In addition the following penal sanctions may be imposed:

Anyone who fails to notify the DPA of the establishment or the operation of a file or any change in the terms and conditions regarding the granting of the permit will be punished by imprisonment for up to three years and a fine amounting between EUR 2,940 and EUR 14,705.

Anyone who keeps a file without permit or in breach of the terms and conditions referred to in the DPA's permit, will be punished by imprisonment for a period of at least one year and a fine amounting between EUR 2,940 and EUR 14,705.

Anyone who proceeds to the interconnection of files without notifying the DPA accordingly will be punished by imprisonment for up to three years and a fine amounting between EUR 2,940 and EUR 14,705. Anyone who proceeds to the interconnection of files without the DPA's permit, wherever such permit is required, or in breach of the terms of the permit granted to him, will be punished by imprisonment for a period of at least one year and a fine amounting between EUR 2,940 and EUR 14,705.

Anyone who unlawfully interferes in any way whatsoever with a personal data file or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment and a fine and, regarding sensitive data, by imprisonment for a period of at least one year and a fine amounting between EUR 2,940 Euros and EUR 29,411, unless otherwise subject to more serious sanctions.

Any data controller who does not comply with decisions issued by the DPA in the exercise of the right of access, in the exercise of the right to object, as well as with acts imposing the administrative sanctions will be punished by imprisonment for a period of at least two years

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

and a fine amounting between EUR 2,940 and EUR 14,705. The sanctions referred to in the preceding sentence will also apply to any data controller who transfers personal data, in breach of the Law.

If the data controller is not a natural person, then the representative(s) of the legal entity shall be liable.

Finally, any natural person or legal entity of private law, who in breach of the Law, causes material damage will be liable for damages in full. If the same causes non pecuniary damage, s/he will be liable for compensation. Liability subsists even when said person or entity should have known that such damage could be brought about. The compensation payable according to article 932 of the Civil Code for non-pecuniary damage caused in breach of the Law has been set at the amount of at least EUR 5,882, unless the plaintiff claims a lesser amount or the said breach was due to negligence. Such compensation shall be awarded irrespective of the claim for damages.

ELECTRONIC MARKETING

Electronic marketing is regulated by Law 3471/2006 "*for the protection of personal data and privacy in electronic communications*" (**"The Law"**), in combination with the general provisions of Law 2472/1997 "for the protection of individuals from the processing of personal data" (**"The Data Protection Act"**).

According to the provisions of article 11 of the Law, data processing for electronic marketing purposes is allowed only upon the individuals' prior express consent. The said article prohibits the use of automated calling systems for marketing purposes to subscribers that have previously declared to the public electronic communications services providers ("CSPs") that they do not wish to receive such calls in general. The CSPs must register these declarations for free on a separate publicly accessible list.

Personal data (such as e-mail addresses) that have been legally obtained in the course of sales of products, provision of services or any other transaction may be used for electronic marketing purposes, without the receiver's prior consent thereto, provided that the receiver of such email has the possibility to "opt out" for free to the collection and processing of his/her personal data for the aforementioned purposes.

Direct marketing emails or advertising emails of any kind are absolutely prohibited, when the identity of the sender is disguised or concealed and also when no valid address, to which the receivers can address requests for the termination of such communications, is provided.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Articles 4 and 6 of the Law (as amended by Directive 2009/136/EC) deals with the collection of location and traffic data by CSPs and the use of cookies and similar technologies.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Traffic data – Traffic data of subscribers or users held by a CSP must be erased or anonymised after the termination of a communication, unless they are retained for one the following reasons:

- The billing of subscribers and the payment of interconnections, provided that the subscribers are informed of the categories of traffic data that are being processed and the duration of processing, which must not exceed 12 months from the date of the communication (unless the bill is doubtable or unpaid).
- Marketing of electronic communications services or value added services, to the extent that traffic data processing is absolutely necessary and following the subscriber's or the user's prior express consent thereto, after his/her notification regarding the categories of traffic data that are being processed and the duration of the processing. Such consent may be freely recalled. The provision of electronic communication services by the CSP must not depend on the subscriber's consent to the processing of his/her traffic data for other purposes (eg. Marketing purposes).

Location data – Location data may only be processed for the provision of value added service, only if such data are anonymised or with the subscriber's/ user's express consent, to the extent and for the duration for which such processing is absolutely necessary. The CSP must previously notify the user or the subscriber of the categories of location data that are being processed, the purposes and the duration of the processing as well as of the third parties to which the data will be transmitted for value added services provision. The subscriber's/user's consent may be freely recalled and the "opt out" possibility must be provided to the subscriber by the CSP free of charge and with simple means, every time he is connected to the network or in each transmission of communication.

Location data processing is allowed exceptionally without the subscriber's/user's prior consent to authorities dealing with emergencies, such as prosecution authorities, first aid or fire-brigade authorities, when location of the caller is necessary for serving such emergency purposes.

Cookie compliance – The use and storage of cookies and similar technologies is allowed when the subscriber/user has provided his express consent, after his/her comprehensive and detailed notification by the CSP. The subscriber's consent may be provided through the necessary browser adjustments or through the use of other applications.

The latter do not prevent the technical storage or use of cookies for purposes relating exclusively to the transmission of a communication thorough an electronic communications network or the provision of an information society service for which the subscriber or the user has specifically requested. The Data Protection Authority is the competent authority for the issuance of an Act, which will regulate the ways such services will be provided and the subscribers' consent will be declared.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

22. HONDURAS

CONTRIBUTION DETAILS

Julio Alejandro Pohl García Prieto
Associate

julio.pohl@gufalaw.com
Bufete Gutiérrez Falla y Asociados
Avenida La Paz, # 2702, Tegucigalpa, Honduras
T +504 2238-2455

LAW

Personal Data Protection is regulated mainly in:

1) **National Constitution**: Article 182 provides the constitutional protection of Habeas Data, giving individuals the right "to access any file or record, private or public, electronic or hand written, that contains information which may produce damage to personal honour and family privacy. It is also a method to prevent the transmission or disclosure of such data, rectify inaccurate or misleading data, update data, require confidentiality and to eliminate false information. This guarantee does not affect the secrecy of journalistic sources."

2) **Law of the Civil Registry** (Article 109, Decree 62-2004). This Law refers only to public personal information that is contained in the archives of the Civil Registry.

3) **Law for Transparency and for Access to Public Information** (Article 3.5, Decree 170-2006). This law enables the access of any person to all the information contained in public entities, except that which is classified as "Confidential." It also extends the Constitutional Protection of Habeas Data and forbids the transmission of personal information that may cause any kind of discrimination or any moral or economical damage to people.

DEFINITION OF PERSONAL DATA

Public Personal Data under the Law of the Civil Registry is: "Public data whose disclosure is not restricted in any way, and includes the following: (a) names and surnames; (b) ID number; (c) date of birth and date of death; (d) gender; (e) domicile (but not address); (f) job or occupation; (g) nationality; and (h) civil status."

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive Personal Data in the Law for Transparency and for Access to Public Information is defined as: "Those personal data relating to ethnic or racial origin, physical, moral or emotional characteristics, home address, telephone number, personal electronic address, political

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

participation and ideology, religious or philosophical beliefs, health, physical or mental status, personal and familiar heritage and any other information related to the honour, personal or family privacy, and self-image."

Other Definitions:

Consent: Written and express authorization of the person to whom the personal data refers in order to disclose, distribute, commercialise, and/or use it in a different way as it was originally given for.

Confidential Information: Information provided by particular persons to the Government which is declared confidential by any law, including sealed bids for public tenders.

Classified Information: Public information classified as that by the law, and/or by resolutions issued by governmental institutions.

NATIONAL DATA PROTECTION AUTHORITY

Two entities protect personal data:

1) National Civil Registry (http://www.rnp.hn).

2) Institute for the Access to Public Information (http://www.iaip.gob.hn).

REGISTRATION

Only "Obligated Entities" must inform the Institute for the Access to Public Information of their databases. Obligated Entities are: (a) government institutions, (b) NGO's, (c) entities that receive public funds and (d) trade unions with tax exemptions.

The Institute for the Access to Public Information will maintain a list of the databases of the above-mentioned entities.

DATA PROTECTION OFFICERS

Only Obligated Entities must appoint a data protection officer.

COLLECTION AND PROCESSING

Individuals, companies, and/or Obligated Entities that because of their work collect personal data may not use sensitive personal data or confidential information without the consent of the person to whom such information refers.

However, consent is not required to use or transfer personal data in the following cases:

- if the information is used for statistical or scientific needs, but only if the personal data is provided in a way that it cannot be associated with the individual to whom it relates;
- if the information is transmitted between Obligated Entities, only if the data is used in furtherance of the authorised functions of those entities;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- If ordered by a Court;
- If the data is needed for the purpose it was provided to the individual or company to perform a service. Such third parties may not use personal information for purposes other than those for which it was transferred to them; and
- 5. In other cases established by law.

TRANSFER

Individuals and/or companies may not transfer, commercialize, sell, distribute or provide access to personal data contained in databases developed in the course of their job, except with the express and direct written consent of the person to whom that data refers, subject to the exceptions set forth above.

SECURITY

The Institute for the Access to Public Information has the authority to enforce all obligated entities to take necessary security measures for the protection of the personal data they collect and/or use.

The Law neither clarifies nor specifically identifies the security policies or security mechanisms that Obligated Entities must comply with.

As a general statement, the Institute for the Access to Public Information has to warrant the Security of all Public Information, of all information classified as confidential by public entities, of all sensitive personal data, and of all information to which the Law gives a secrecy status.

BREACH NOTIFICATION

Breach notification is not required.

ENFORCEMENT

The Institute for the Access to Public Information may receive complaints of abuses regarding the collection of personal or Confidential Data.

The Institute will impose corrective measures and establish recommendations for those persons or companies who disclose Personal Data, Sensitive Personal Data or Confidential Data without authorization.

ELECTRONIC MARKETING

There is no law in relation to electronic marketing, nor any regulation on this subject.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no law in relation to this issue, nor any regulation on this subject.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

23. HONG KONG

CONTRIBUTION DETAILS

Matthew Glynn
Partner – Head of IPT Asia
Managing Director and Country Managing Partner – Singapore
T +65 6512 9595 (Singapore)
T +852 9634 8999 (Hong Kong)
matt.glynn@dlapiper.com

Arthur Cheuk
Associate
T +852 2103 0501
arthur.cheuk@dlapiper.com

LAW

The Personal Data (Privacy) Ordinance (Cap. 486) ("**Ordinance**") regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data ("**PCPD**").

The Ordinance was recently amended by the Personal Data (Privacy) (Amendment) Bill ("**Bill**") in July 2012. Most of the amendments introduced by the Bill came into force on 1 October 2012. However, two major areas, namely new restrictions against the use and provision of personal data in direct marketing and new powers of the PCPD to provide legal assistance to persons in civil proceedings, are not in force at the time of writing (but are expected to come into force in 2013).

DEFINITION OF PERSONAL DATA

"Personal Data" is defined in the Ordinance as any data:

- relating directly or indirectly to a living individual;
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- in a form in which access to or processing to the data is practicable.

DEFINITION OF SENSITIVE PERSONAL DATA

The concept of sensitive personal data does not apply in Hong Kong.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Privacy Commissioner for Personal Data
12/F, 248 Queen's Road East
Wanchai
Hong Kong
T +852 2827 2827
F +852 2877 7026
http://www.pcpd.org.hk/

The PCPD is responsible for overseeing compliance with the Ordinance.

REGISTRATION

Currently, there is no requirement for the registration of data users in Hong Kong.

However, under the Ordinance the PCPD has the power to specify certain classes of data users to whom registration and reporting obligations apply. Under the Data User Return Scheme ("**DURS**"), data users belonging to the specified classes are required to submit data returns containing prescribed information to the PCPD, which will compile them into a central register accessible by the public. However, at the time of writing, no register has been created to date. The PCPD has proposed to implement the DURS in phases, with the initial phase covering data users from the following sectors and industries:

- the public sector;
- banking, insurance and telecommunications industries; and
- organisations with a large database of members (e.g. customer loyalty schemes).

A public consultation for the DURS by the PCPD was concluded in September 2011. The PCPD had originally planned to implement the DURS in the second half of 2013 but the exact time-frame for implementation has yet to be announced.

DATA PROTECTION OFFICERS

Currently, there is no requirement for data users to appoint a data protection officer in Hong Kong.

COLLECTION AND PROCESSING

A data user may collect personal data from data subjects if:

- the personal data is related to a function of the data user;
- the collection is necessary, lawful and fair;
- the data collected is not excessive; and
- the data user has been informed of the following:
  - whether the provision of personal data by data subjects is mandatory and the consequence(s) for not supplying the data;
  - the purposes for which the data will be used;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the persons to whom the data may be transferred;
- the data subjects' right to request for access and/or correction their personal data; and
- the contact details of the person to whom requests for access or correction should be sent.

Data users may only use and process personal data for purposes for which the data was collected. Any usage of personal data for new purposes requires the prescribed consent of the data subject concerned.

TRANSFER

Data users may not transfer personal data to third parties, unless the data subjects have been informed of the following before their personal data was collected:

- that their personal data may be transferred; and
- the classes of persons to whom the data may be transferred.

There are currently no restrictions for transfer of personal data outside of Hong Kong. Although such restrictions are set out in the Ordinance, they are currently not in force.

SECURITY

Data users are required by the Ordinance to take all practicable steps to protect personal data against unauthorised or accidental access or loss. The steps which are considered appropriate depend on the nature of the personal data and the harm that could result if data breaches or leaks were to occur.

Under the new amendments to the Ordinance, where the data user engages a data processor to process personal data on its behalf, the data user must use contractual or other means to:

- prevent unauthorised or accidental access, processing, erasure, loss of use of the personal data; and
- ensure that the data processor does not retain the personal data for longer than necessary.

BREACH NOTIFICATION

Currently, there is no mandatory requirement for data users to notify authorities or data subjects about data breaches in Hong Kong.

ENFORCEMENT

The PCPD is responsible for enforcing the Ordinance. If a data user is found to have contravened the data protection principles of the Ordinance, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Failure to abide by the enforcement notice is a criminal offence, punishable by a fine of up to HK$ 50,000 and imprisonment for up to 2 years. In the case of subsequent convictions, additional and more severe penalties apply. Contravention of other requirements of the Ordinance is also an offence.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

In particular, breach of new provisions relating to direct marketing (which at the time of writing has yet to come into effect) is punishable by a fine of HK$ 1,000,000 and imprisonment of up to 5 years, depending on the nature of the breach.

In addition to criminal sanctions, data subjects aggrieved by contravention of the Ordinance may also seek compensation from the data user through civil action.

ELECTRONIC MARKETING

The Ordinance was amended in 2012 to include, amongst other things, provisions regulating the use and provision of personal data for purposes of direct marketing which may be conducted by any means (electronic or otherwise). These provisions are expected to come into effect some time in 2013.

The new amendments generally require data users who wish to either use or provide personal data for direct marketing purposes to make specific disclosures to the data subjects and obtain consents for such actions. The disclosures include:

- a statement of intention to use/provide their personal data for direct marketing;
- a statement that the data user may not use/provide the personal data without the data subjects' consent;
- a dedicated channel via which the data subjects may give such consent;
- the kind(s) of personal data to be used/provided;
- the class(es) of persons to whom the personal data may be provided;
- the class(es) of goods/services to be direct marketed; and
- a statement that the personal data may be provided for gain, if applicable.

Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received. In addition, when data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt-out at any time, free of charge.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The principles as stated in the Ordinance also apply in the online environment. For example, under the Ordinance, data users have the obligation to inform data subjects of the purposes for collecting their personal data. If a website uses cookies to collect personal data from its visitors, this should be made known to them. Data users should also inform the visitors whether and how non-acceptance of the cookies will affect the functionality of the website.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

24. HUNGARY

CONTRIBUTION DETAILS

Zoltán Kozma
Counsel
T +36 1 510 1100
zoltan.kozma@dlapiper.com

LAW

The EU Data Protection Directive 95/46/EC is currently implemented in Hungary by Act No. CXII of 2011 on Informational Self Determination and Freedom of Information which came into force on 1 January 2012 ("**Act**"). Enforcement is through the National Authority for Data Protection and Freedom of Information ("**Authority**").

DEFINITION OF PERSONAL DATA

Personal data shall mean any data relating to the data subject – in particular name, identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity – and any reference that can be drawn from such data in respect of the data subject. In the course of data processing, such data shall be treated as personal data as long as the connection between the data and the data subject remains restorable. The data shall be considered subject to restoration, if the data controller bears the technical measures necessary for such restoration. Unless the data controller is directly able, by its technical capabilities, to trace the data back to the data subject, data shall not be considered as "personal data". This so called "relative" nature of personal data, which in practice narrows the meaning of personal data, is only present in a few jurisdictions.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data shall mean:

- personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade union membership or sex life; and
- personal data concerning health, addictions, or criminal personal data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

National Authority for Data Protection and Freedom of Information
Address: H-1125 Budapest, Szilágyi Erzsábet fasor 22/c.
T +36 1 391 1400
F +36 1 391 1410
http:\\www.naih.hu
ügyfélszolgálat@naih.hu

REGISTRATION

If a data controller intends to conduct data processing, it is obliged to file a request with the Authority. Data processing must be registered by the Authority before it can occur. The Authority will charge a fee for registration. The fee that will be charged is currently unknown, but is expected to fall within the range of EUR 20-30.

Should the Authority fail to respond to a request for registration within 8 days of the filing of such a request, data processing may be commenced.

No register is held and thus no request can be filed for processing personal data relating to data subjects employment, membership, or customer relationship with the data controller. Financial institutions, community service providers and electronic communication service providers are excluded from this exemption, i.e. they will be obliged to register even if they process the above data.

The notification should include the following information:

- the purpose of processing;
- the types of data and the grounds for processing;
- the categories of data subjects;
- the source;
- the categories of data transferred, the recipients and the grounds for transfer;
- the name and registered office of the data controller and the data processor, the place where records are stored and/or where processing is carried out, and the data processor's activities in connection with data processing operations;
- the name and contact information for the internal data protection officer (if any); or
- the applied technology for data processing.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DATA PROTECTION OFFICERS

The following data controllers and data processors shall appoint or commission an internal data protection officer ("**DPO**") (holding a law degree, a degree in economics or computer sciences or an equivalent degree in higher education) who is to report directly to the head of the organisation:

- authorities that control or process personal data in respect of nationwide registers, or authorities that control or process employment or criminal records;
- financial institutions; and
- telecommunications service providers and public utility companies.

As a new institution effective from 1 January 2012, the head of the Authority will convene a conference of the DPOs at least once a year to discuss data protection related matters.

COLLECTION AND PROCESSING

Personal data may be collected and processed if;

- the data subject has given his or her consent, or
- this is required by an Act or by a decree of the local municipality based on the authorisation conferred by an Act concerning the specific data as defined therein.

Personal data can also be processed if it is impossible to obtain the consent of the data subject or it would cause disproportionate costs and the processing is necessary;

- for compliance with a legal obligation to which the controller is subject; or
- for the purposes of the legitimate interests of a third party, or the controller itself, where the assertion of such interests is proportionate with the interference in data protection rights.

Sensitive data may be processed if;

- the data subject has given his or her explicit consent in writing, or
- it is necessary to enforce an obligation prescribed by an international treaty, or for the enforcement of a constitutional right set forth in the Fundamental Law of Hungary, or prescribed by an Act for national security or law enforcement purposes regarding personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade union membership or sex life; or
- the data is required by an Act for the purpose of public order in the case of personal data concerning health, addictions, or criminal personal.

Personal data may be processed only for specified and explicit purposes, where it is necessary for exercising certain rights or fulfilling certain obligations. This purpose must be satisfied in all stages of operations of data processing.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The personal data processed must be essential for the purpose for which it was collected, it must be suitable to achieve that purpose, and it may be processed to the extent and the duration necessary to achieve that purpose.

TRANSFER

Transferring personal data of data subjects within the EEA shall be considered as data transfer within Hungary. Transferring personal data to data processors within the EEA is possible without the consent of the data subjects. Under the Act a data processor is the person that is engaged in the processing of personal data on behalf of the controller, and the data processor is carrying out "the technical operations in connection with the data management." In practice an entity will be a data processor for the purposes of the Act where it acts on the basis of the instructions (on behalf) of the data controller and follows the predetermined rules and methodology set by the data controller.

The Act makes it possible to transfer personal data to third countries (ie to countries outside of the EEA) if the conditions (legal bases) of the data processing are satisfied (see above) and adequate level of protection is afforded in such third countries.

SECURITY

Data controllers, and within their sphere of activity, data processors must ensure personal data protection and must implement technical and organisational measures, as well as adequate procedural rules to enforce the provisions of the Act and other regulations concerning confidentiality and security of data processing.

Personal data must be protected against unauthorised access, alteration, transfer, disclosure, deletion, accidental deletion or damage as well as against being unable to access the data due to the change in the applied technology.

If multiple possibilities for data processing solutions exist, the solution to be chosen should provide a higher level of security for personal data, unless this would result in a disproportionate burden for the data controller.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the Commissioner or to data subjects.

As an exception rule, however, electronic communication service providers must immediately report data security breaches to the National Media and Infocommunications Authority under Act No. 100 of 2003 on Electronic Communications.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

As mentioned above the new Act introduced the so-called National Authority for Data Protection and Freedom of Information, an administrative body replacing the Commissioner. The leader of the Authority is the President, nominated by the Prime Minister and appointed by the President of the Republic, for a total term of 9 years. The Authority will have broader powers than the Commissioner before it.

The new Authority takes over the role of the Commissioner, but with greater powers. It will have the power necessary to ensure and enforce compliance with data protection laws. The newly created procedures of the Authority will be more differentiated and thorough and might consist of several phases, in accordance with the provisions of the new Act. These procedures will provide more effective tools for the Authority to protect the rights of the data subjects in connection with the processing of their personal data by data controllers.

The Authority will have several instruments to enforce compliance, the most important being:

- ordering the correction of inadequate personal data;
- ordering the block deletion or termination of illegally controlled personal data;
- prohibiting the illegal controlling or processing of personal data;
- prohibiting the transfer of personal data to foreign countries;
- ordering the notification of the affected party, if the data controller illegally refused to do so;
- imposing a fine ranging from HUF 100,000 (cca. EUR 350) to 10,000,000 (cca. EUR 35,000).

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be "personal data" for the purposes of the Act).

Also, pursuant to Act 48 of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (hereinafter referred to as "direct marketing"), such as through electronic mail or equivalent individual communications only upon the express prior consent of the person to whom the advertisement is addressed. The request for the consent may not contain any advertisement, other than the name and description of the company.

The statement of consent may be made in any way or form, on condition that it contains the name of the person providing it, and – if the advertisement to which the consent pertains may be disseminated only to persons of a specific age – his place and date of birth, furthermore, any other personal data authorised for processing by the person providing the statement, including an indication that it was given freely and in possession of the necessary legal information.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The statement of consent may be withdrawn freely any time, free of charge and without any explanation. In this case all personal data of the person who has provided the statement must be promptly erased from the records and all advertisements must be stopped.

Pursuant to Act 100 of 2003 on Electronic Communications ("EC Act"), applying automated calling system free of any human intervention, or any other automated device for initiating communication in respect of a subscriber for the purposes of direct marketing, providing information, public-opinion polling and market research shall be subject to the prior consent of the subscriber.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The EC Act deals with the collection of location and traffic data by public electronic communications services providers ("**CSPs**") and use of cookies (and similar technologies).

Traffic Data – With certain special exceptions set out in the EC Act (e.g. invoicing, collecting subscriber fees, law enforcement, national security and defence), traffic data relating to subscribers and users processed and stored by CSPs while providing such services must be erased or made anonymous when it is no longer needed.

CSPs may use certain traffic data as referred to in the EC Act for the provision of value added services or for marketing purposes subject to the subscriber's or user's prior consent, to the extent necessary for the provision of such services or for marketing purposes. CSPs shall provide the possibility for users or subscribers to withdraw their consent at any time.

Location Data – CSPs shall be authorised to process location data only upon the prior consent of the subscribers or users to whom the data are related, and only to the extent and for the duration as it is necessary for the provision of value added services.

Users and subscribers shall have the right to withdraw their consent at any time.

CSPs shall be required to comply with any request for location information in connection with specific subscribers or users, if made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, to the extent required to discharge their respective duties.

Cookie Compliance – Pursuant to the EC Act, on the electronic communication terminal equipment of a subscriber or user, information may be stored, or accessed, only upon the user's or subscriber's prior consent granted in possession of clear and comprehensive information, which information inter alia includes the purpose of processing.

The competent Hungarian Authorities have not issued any guidance in respect of the interpretation of "consent" and the manner how this consent should be obtained in practice. General practice is that consent can be obtained via browser settings, however, as mentioned so far this has not been confirmed by the opinion or the guidance of the Authorities yet.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

25. INDIA

CONTRIBUTION DETAILS

Vakul Corporate Advisory Pvt. Ltd. (Law Firm)

Vakul Sharma
Managing Partner
T +91 11 47025460
vakul@sify.com

Seema Sharma
Senior Partner
T +91 11 47025460
seekat@sify.com

LAW

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act, 2000 (the "**Act**") contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically).

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("**Privacy Rules**"). The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information', as defined below.

In August 2011, India's Ministry of Communications and Information issued a "Press Note" Technology (*Clarification on the Privacy Rules*), which provided that any Indian outsourcing service provider/organisation providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is **not** subject to collection & disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects ("**providers of information**") when providing their services.

DEFINITION OF PERSONAL DATA

The Privacy Rules define the term "personal information" as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

The Privacy Rules define "sensitive personal data or information" to include the following information relating to:

- password;
- financial information e.g. bank account/credit or debit card or other payment instrument details;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- (biometric information;
- any detail relating to the above clauses as provided to a corporate entity for providing services; and
- any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

NATIONAL DATA PROTECTION AUTHORITY

No such authority exists.

REGISTRATION

No requirements.

DATA PROTECTION OFFICERS

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests.

COLLECTION AND PROCESSING

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The Privacy Rules state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information. However, the August 2011 "Press Note" issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication.

The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information including sensitive personal information and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf). Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following at the time of collection of sensitive personal information or other personal information: (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of the agency that is collecting the information and the agency that will retain the information.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (i.e. she will be able to withdraw his/her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

TRANSFER

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer, if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offence for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Thus, contracts should also specifically include provisions (a) entitling the data collector to distinguish between 'personal information' and 'sensitive personal information' that it wishes to collect/process; (b) representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information; and (c) outlining the liability of the third party.

SECURITY

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement "reasonable security practices and procedures" to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Federal Government.

BREACH NOTIFICATION

There is no mandatory requirement under the Act or Privacy Rules to report data security breaches. However, a corporate entity can be asked to furnish information to the Indian Computer Emergency Response Team (CERT-IN) related to cyber security incidents.

ENFORCEMENT

Civil penalties of up to EUR 694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount.

Criminal penalties of up to 3 years imprisonment or a fine up to EUR 6,950, or both for unlawful disclosure of information.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

The Act does not refer to electronic marketing directly. However, sending false information (emails, SMS, MMS, etc.) persistently by means of a computer resource or a communication device for the purpose of causing annoyance, inconvenience, etc. is punishable under Indian law. Further, such emails, SMS, MMS etc. must not disguise or conceal the identity of the sender.

The Privacy Rules also provide the right to "opt out" of email marketing, and the company's privacy policy must address marketing and information collection practices.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no regulation of cookies, behavioural advertising or location data.

However, the IT Act contains both civil and a criminal offenses for a variety of computer crimes:

- Any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to EUR 694,450 (by an Adjudicating Officer); damages in a civil suit may exceed this amount. Under the IT Act, "computer contaminant" is defined as any set of computer instructions that are designed (a) to modify, destroy, record, or transmit data or programmes residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system or computer network;
- Any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to 3 years and fine up to EUR 1,390.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

26. INDONESIA

CONTRIBUTION DETAILS

K&K Advocates – Intellectual Property
BRI Building II, Fl. 15, Suite 1502
Jl. Jend. Sudirman Kav.44-46
Jakarta 10210 – Indonesia
T +62 21 5785 0331
F +62 21 5785 3107
www.kk-advocates.com

Justi Kusumah (Managing Partner)
justi.kusumah@kk-advocates.com

Risti Wulansari (Partner)
risti.wulansari@kk-advocates.com

Atiya Arifah (Associate)
atiya.arifah@kk-advocates.com

LAW

Specific Regulations

Law No. 11 of 2008 regarding Electronic Information and Transaction (the "**EIT Law**") and the recently issued the Government Regulation No. 82 of 2012 regarding Provision of Electronic System and Transaction ("**Reg. 82**"), which just came into force on 15 October 2012.

Prior to promulgation of Reg. 82, provisions regulating data protection and/or collection of personal data/personal information were scattered under various regulations.

In addition to the provisions under EIT Law and Reg. 82, there are also a series of regulations which also cover certain provisions which may relate to data protection, such as:

- Telecommunications Sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications (the "**Telecommunications Law**") provides that any person is prohibited from any kinds of tapping on information transmitted through any kinds of telecommunications network. Furthermore, Article 42 of the Telecommunications Law stipulates that any telecommunications services operator has to keep confidential any information transmitted and/or received by telecommunications service subscriber through telecommunications networks and/or telecommunications services provided by the relevant operator.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Public Information Sector

Article 6 of Law No. 14 of 2008 regarding Disclosure of Public Information provides that any information relating to personal rights is prohibited from distribution by public agencies or entities. Furthermore, Article 17 of the relevant law also prohibits the disclosure of private information of any person, particularly which concerns family history; medical and psychological history; financial information (incluing assets, earnings and bank records); evaluation records concerning a person's capability/recommendation/intellectual, formal/informal education records.

- Banking and Capital Markets Sectors

Data privacy in this sector is regulated under Law 7 of 1992 as amended by Law 10 of 1998 on Banking ("**Banking Law**") and Law 8 of 1995 on Capital Markets ("**Capital Markets Law**") respectively. The regulations apply to both individuals and corporate data.

Bank Indonesia's Regulation No. 7/15/PBI/2007 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank stipulates that the bank's customer data transfer (by way of establishing a data centre or a data processing outside Indonesia territory) necessitates prior approval being obtained from Bank Indonesia.

In addition, the transfer of the bank's customer data for purposes other than banking transactions requires the customer's prior consent.

DEFINITION OF PERSONAL DATA

Reg. 82 defines personal data as: data of an individual, which is stored, kept, and of which its confidentiality and truth is maintained.

DEFINITION OF SENSITIVE PERSONAL DATA

Currently, there is no specific definition on sensitive personal data under the prevailing laws and regulations.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority for data privacy in general in Indonesia.

The Capital Markets and Financial Bodies Supervisory Body ("**Bapepam LK**") acts as regulator of data privacy in the capital markets sector.

Bank Indonesia also acts as the regulator with regard to banks' customer data privacy issues.

REGISTRATION

Indonesia does not maintain a register of controllers or of processing activities.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

According to general law principles, data controllers may collect and process personal data when any of the following conditions are met:

- the data subject consents;
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party;
- the processing satisfies the data controller's legal obligation;
- the processing is required by the Government of Indonesia or by law, or to perform a public function in the public interest, or to administer justice; or
- the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests.

Both EIT Law and Reg. 82 specifically regulate the obligation to obtain "consent" from the owner of a personal data in the case of data collection, use and processing.

Reg. 82 provide the specific provisions on the obligation to set up a data centre in Indonesia, namely:

- Before an Electronic System is implemented, the provider of an Electronic System has to obtain a Electronic certificate from the Ministry of Communication, Information and Technology ("MCIT").
- In providing the provision of an Electronic System, the provider should certify that its Electronic System is secure, continuous, and that the personal data obtained, used and utilised is based on the owner's prior consent and that the disclosure of the personal data is conducted in accordance with the owner's prior consent and is in line with the objectives as disclosed to the relevant owner.
- The provider of the Electronic System is also obliged to provide audit track records.

TRANSFER

Reg. 82 regulates the transfer of data in Article 22 which provides that in any case that electronic information and/or electronic document is transferred, the provider has to explain the control and possession of the electronic information and/or electronic document.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

The obligations of Electronic System Providers are regulated under Reg. 82 and amongst other things:

- Guarantee the confidentiality of the source code of the software (Article 9);
- Ensure agreements on minimum service level and information security as well internal communication security (Article 12);
- Protect and ensure the privacy and personal data protection of users (Article 15);
- Ensure the appropriate lawful use and disclosure of the personal data (Article 15);
- Provide data centre and disaster recovery centre (Article 17);
- Provide the audit records on all Provision of Electronic Systems activities (Article 18); and
- Provide information in the Electronic System based on legitimate request from investigators for certain crimes (Article 29).

On the telecommunication sector, Article 19 of Minister of Communication and Informatics Regulation No. 26/PER/M.KOMINFO/05/2007 regarding the Security and Utilisation of Internet Protocol-based Telecommunications Network ("**MR 26/2007**") also provides that the telecommunication service provider is responsible for data storage due to its obligation to record its log file for at least 3 months.

BREACH NOTIFICATION

Article 15 Paragraph 2 of Reg. 82 provides that the provider of a Electronic System must provide written notification to the owner of personal data, upon its failure to protect the personal data.

Article 20 Paragraph 3 of Reg. 82 provides that the provider of Electronic System must make the utmost effort to protect personal data and to immediately report any failure/serious system interference/disturbance to a law enforcement official or Supervising Authority of telecommunications sector.

ENFORCEMENT

In Indonesia, the sanctions for breaches of data privacy are found under the relevant legislation and are essentially fines. Imprisonment may be imposed in severe instances such as in the event of intentional infringement.

- The EIT Law provides criminal penalties ranging from; Rp. 600,000,000 fine to Rp. 800,000,000 and/or 6 to 8 years imprisonment for unlawful access; Rp. 800,000,000 fine and/or 10 years imprisonment for interception/wiretapping of transmission; to Rp. 2,000,000,000 to Rp. 5,000,000,000 and/or 8 to 10 years imprisonment for alteration, addition, reduction, transmission, tampering, deletion, moving, hiding Electronic Information and/or Electronic Records.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Failure to comply with Reg. 82 is subject to administrative sanctions (which do not eliminate any civil and criminal liability). These administration sanctions are in the forms of:
  - Written warning;
  - Administrative fines;
  - Temporary dismissal; and/or
  - Expelled from the list of registrations (as required under the regulation).
- Banking Law

Under Article 44 of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept secret may be sentenced to imprisonment for not less than two years but not more than four years, and fined at least four billion but not more than eight billion Indonesian Rupiah.

- Capital Markets Law

Under Capital Markets Law, the Capital Market and Financial Institutions Regulatory Body (BAPEPAM LK is empowered to impose the following administrative sanctions for breaches of the provisions dealing with data protection). The sanctions comprise:

- a written reminder;
- a fine;
- limitations on business;
- suspension of business;
- revocation of business licence;
- cancellation of approval;
- cancellation of registration; or
- ET Law.

ELECTRONIC MARKETING

EIT Law and Reg. 82 do not specifically address electronic marketing.

Article 25 of the EIT Law provides that Internet website, amongst other things, is acknowledged and protected as an Intellectual Property (IP) and consequently, should fall under the ambit of the relevant IP laws, which may in certain cases fall under the Indonesian Copyright Law.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is currently no laws and regulations concerning cookies and location data.

However, if the data collected by cookies or location data is obtained from by the unlawful access of another party's electronic information, this is subject to 6 to 8 years imprisonment and/or a fine of Rp. 600,000,000 to Rp. 800,000,000.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

27. IRELAND

CONTRIBUTION DETAILS

Mason Hayes & Curran
www.mhc.ie

Philip Nolan
Partner and Head of Commercial Department
T +353 1 6145078
pnolan@mhc.ie

LAW

The core Irish data protection law is comprised in the Data Protection Act 1988 ("**1988 Act**") as amended by the Data Protection (Amendment) Act 2003 ("**2003 Act**") (together the Data Protection Acts ("**DPA**")). The 2003 Act implemented the EU Data Protection Directive (95/46/EC). In addition to the DPA, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ("**ePrivacy Regulations**") set out data protection rules in relation to direct marketing and electronic networks and services, including location data and cookies.

DEFINITION OF PERSONAL DATA

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

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data means personal data as to:

- the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;
- whether the data subject is a member of a trade union;
- the physical or mental health or condition or sexual life of the data subject;
- the commission or alleged commission of any offence by the data subject; or
- any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Office of the Data Protection Commissioner ("**DPC**")

Canal House
Station Road
Portarlington
Co. Laois
Ireland
LoCall 1890 25 22 31
T +353 57 868 4800
F +353 57 868 4757
info@dataprotection.ie
www.dataprotection.ie

REGISTRATION

All data controllers and data processors are required to register with the DPC unless exempt.

The Irish registration regime contains wide exemptions for certain categories of processing that do not trigger a registration obligation. There are also certain categories of data controller and data processor that are subject to an absolute obligation to register.

The DPA exempts:

- not for profit organisations, provided they only process personal data relating to their activities;
- data controllers and data processors who process personal data kept in a public register; and
- data controllers and data processors who only process manual data.

The Data Protection Act 1988 (Section 16(1)) Regulations 2007 ("**2007 Regulations**") also exempt from registration:

- data controllers that only process employees' human resources data in the normal course of personnel administration;
- candidates for political office and elected representatives;
- schools, colleges, universities and similar educational institutions;
- solicitors and barristers;
- data controllers who process customer and supplier data in the context of normal commercial activity;
- companies who process personal data of past and present shareholders, directors or other officers in complying with the Irish Companies Acts;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- data controllers who process personal data for the purpose of publishing journalistic, literary or artistic material; and
- data controllers or data processors who operate under a statutory data protection code of practice.

Data processors that process personal data on behalf of any of the above categories of data controller are also not required to register.

The 2007 Regulations impose an absolute obligation to register on banks, insurance undertakings, direct marketing firms, debt collection agencies, credit reference agencies, health professionals, anyone processing genetic data, ISPs and telecoms companies. Any data processor that processes personal data on behalf of a data controller that falls into one of these categories is also obliged to register. A failure by a data controller or processor to register, when required to do so, is an offence punishable by fines up to EUR€100,000.

Data controllers and/or data processors are obliged to renew their registration annually. The DPC may refuse an application for registration under certain conditions. There is a right of appeal against a refusal to the Circuit Court.

DATA PROTECTION OFFICERS

There is no legal requirement to appoint a data protection officer but it would be best practice to do so. The DPC recommends that data controllers appoint a co-ordinator to deal with subject access requests. Where a data protection officer is appointed, this information should be supplied to the data subjects. A nominated contact for subject access requests also needs to be provided when making a registration application.

COLLECTION AND PROCESSING

The DPA transposes the data protection principles from the Data Protection Directive, which need to be complied with in relation to the collection and processing of personal data.

In addition to complying with the data protection principles, all processing of personal data must comply with one of a number of legitimate processing conditions contained in the DPA.

These include that:

- the data subject has given his or her consent to such processing;
- the processing is required for the performance of a contract to which the data subject is a party;
- the processing is to prevent an injury or other damage to the health of the data subject;
- the processing is to protect an individual's vital interests;
- the processing is for the administration of justice; or
- the processing is for the purposes of the legitimate interests pursued by a data controller.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

If sensitive personal data is being processed, then an additional set of processing conditions need to be satisfied. These include the "explicit" consent of the data subject. The grounds for processing sensitive data are quite restrictive and it can sometimes be difficult to legitimise the processing of sensitive personal data.

TRANSFER

The DPA contains a number of restrictions on the transfer of personal data by a data controller to a country or territory outside of the European Economic Area ("**EEA**"). Under the DPA, such transfers may not take place unless the receiving country ensures an adequate level of protection for the privacy of data subjects in relation to the processing of their personal data. A limited number of countries are recognised by the by the European Commission as having this level of protection.

Otherwise under the DPA, it is only possible to transfer personal data outside the EEA if:

- the data subject has consented to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data controller;
- the transfer is necessary for reasons of public interest;
- the transfer is necessary under some international obligation of the State;
- the transfer is required or authorised by law;
- the transfer is necessary for obtaining legal advice;
- the transfer is necessary in order to prevent personal injury or damage to the health of the data subject; or
- the transfer is done under one of the EU Approved Model Clauses

Due to the varying standards of data protection in the US, transfers of data from the EEA to the US may take place (in the absence of fulfilling one of the exceptions above) where the recipient in the US has signed up to the Safe Harbour Scheme.

The DPC recognises the use of binding corporate rules, and the Irish DPC has agreed to abide by the mutual recognition procedure. Multinational companies must draft and submit draft BCRs to the DPC for its approval. The Irish DPC acted as the lead authority for approval of the Intel Corporation's BCRs in January 2012.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Data controllers and data processors must take appropriate security measures against unauthorised access to or unauthorised alteration, disclosure or destruction of, personal data, particularly where the processing involves the transmission of data over a network and against all other forms of processing.

As to the level of security required, data controllers and data processors must put in place appropriate security provisions for the protection of personal data, having regard to:

- the current state of technological development;
- the cost of implementing security measures;
- the nature of the personal data; and
- the harm that might result from unauthorised processing or loss of the data concerned.

Data controllers and data processors are also obliged to take all reasonable steps to ensure that their employees and other persons at the place of work concerned are aware of and comply with the relevant security measures.

BREACH NOTIFICATION

The DPC has published a Personal Data Security Breach Code ("**Code**") which states that the DPC must be notified of any unauthorised disclosure of personal data except in limited circumstances. These are where the disclosure:

- affects less than one hundred individuals;
- the loss of sensitive personal or financial data is not involved; and
- the affected individuals have been informed.

Under the ePrivacy Regulations, data breaches in relation to electronic communication networks or services must be notified to the Data Protection Commissioner. Where the breach is likely to affect the personal data or privacy of a subscriber, affected subscribers must also be notified.

In very limited circumstances, data controllers can take the view that affected data subjects do not need to be notified if measures have been taken which will make the data inaccessible to unauthorised users; such technical measures could include encryption.

ENFORCEMENT

The DPC is responsible for the enforcement of the DPA and the ePrivacy Regulations.

A breach of specific provisions of the DPA can result in criminal liability. These include:

- the failure of a data controller or data processor to register;
- the disclosure of personal data which was obtained without authority; and
- the failure to comply with an Enforcement Notice.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Persons found guilty of offences under the DPA may be liable:

- on summary conviction (before a district judge sitting alone), to a fine not exceeding EUR 3,000; or
- on conviction on indictment (before a judge and jury), to a fine not exceeding EUR 100,000.

Breaching other provisions of the DPA do not in themselves give rise to criminal liability, but the DPC may investigate the incident and issue an "Enforcement Notice" compelling a data controller to comply with the DPA. Failure to comply with an Enforcement Notice is an offence.

The ePrivacy Regulations prescribe fines for failure to report data breaches, inadequate security measures and sending of unsolicited communications (spam) with regard to electronic communication networks and services.

In addition to specific penalties arising out of enforcement actions, a breach of the DPA can also give rise to reputational damage, particularly if the DPC publishes details of the breach in his Annual Report or issues a press release (as he does from time to time).

In 2011 the DPC investigated 1,161 complaints (of these, 183 related to a co-ordinated action against one data controller with regard to access rights). This is a record high and represents a sharp increase on the 783 complaints filed in 2010. Approximately 22% of the complaints lodged in 2011 concerned breaches of the ePrivacy Regulations. The remaining 78% related to breaches of the DPA.

Complaints concerning access rights accounted for approximately 48% of the overall total.

ELECTRONIC MARKETING

The ePrivacy Regulations implement the anti-spam rules set out in Article 13 of the Privacy and Electronic Communications Directive (as amended by the Citizens' Rights Directive). These regulations came into effect on 1 July 2011.

Direct marketing emails can generally only be sent to users with their prior consent. A limited exemption is available for direct marketing emails sent to existing customers to promoting other products or services similar to those previously purchased by that consumer (such emails can only be sent for 12 months, the customer must have been given the opportunity to object when the details were collected and the product or service being marketed must be a product or service offered by the person with the existing relationship with the customer)

B2B direct marketing emails can generally be sent unless the recipient has informed the sender that it does not consent to the receipt of such messages.

The identity of the sender must not be disguised or concealed and the recipient must be offered an opt-out.

Direct marketing calls (excluding automated calls) may be made to a landline provided the subscriber has not previously objected to receiving such calls or noted his or her preference not to receive direct marketing calls in the National Directory Database. Direct marketing calls cannot be made to a mobile phone without prior consent.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

One cannot send a direct marketing fax to an individual subscriber in the absence of prior consent. One can send such a fax to a corporate subscriber unless that subscriber has previously instructed the sender that it does not wish to receive such communications or has recorded a general opt-out to receiving such direct marketing faxes in the National Directory Database.

Breach of these anti-spam rules is a criminal offence. On a summary prosecution (before a judge sitting alone) a maximum fine of EUR 5,000 per message sent can be handed down. On conviction on indictment (before a judge a jury) a company may be fined up to EUR 250,000 per message sent and an individual may be fined up to EUR 50,000 per message.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookies – Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The 2011 Regulations expressly refer to the use of browser settings as a means to obtain consent. There is no express requirement for consent to be "prior" to the use of a cookie. A user must be provided with "clear and comprehensive information" about the cookie (including, in particular, its purposes). This information must be prominently displayed and easily accessible. The methods adopted for giving information and obtaining consent should be as "user friendly" as possible.

The DPC has provided regulatory guidance on the use of cookies which can be accessed at: http://www.dataprotection.ie/documents/guidance/Electronic_Communications_Guidance.pdf.

Location Data – One cannot process location data unless either (i) such data has been made anonymous or (ii) user consent has been obtained.

A provider of electronic communication networks or services or associated facilities (i.e. a telco) must inform its users of (i) the type of location data (other than traffic data) that will be processed, (ii) the purpose and duration of the processing and (iii) whether the data will be transmitted to a third party to provide a value added service. Users can withdraw their consent to the processing of location data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

28. ITALY

CONTRIBUTION DETAILS

Giangiacomo Olivi
Partner
T +39 02 80 618 515
giangiacomo.olivi@dlapiper.com

Stefania Baldazzi
Associate
T +39 02 80 618 616
stefania.baldazzi@dlapiper.com

Gianluigi Marino
Associate
T +39 02 80 618 654
gianluigi.marino@dlapiper.com

LAW

The Italian law applicable on privacy issues is the Legislative Decree no. 196 of 30 June 2003 ("*Codice in materia di protezione dei dati personali*", the "**Privacy Code**"). The Privacy Code implements Directives 46/1995/EC and 58/2002/EC.

DEFINITION OF PERSONAL DATA

Pursuant to section 4 of the Privacy Code, "personal data" shall mean any information relating to individuals who are or can be identified, even indirectly, by reference to any other information including a personal identification number.

DEFINITION OF SENSITIVE PERSONAL DATA

Pursuant to Section 4 of the Privacy Code, "sensitive data" shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade unionist character, as well as personal data disclosing health and sex life.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Garante per la protezione dei dati personali (the **"Garante"**).
Piazza di Monte Citorio
n. 121 – 00186 ROMA
T +39 06 696771
F +39 06 69677 3785
www.garanteprivacy.it

REGISTRATION

Pursuant to Section 37 of the Privacy Code, a data controller shall notify the processing of personal data he/she intends to perform exclusively if said processing concerns:

- genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network;
- data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure;
- data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character;
- data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users;
- sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample based surveys;
- data stored in ad hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

DATA PROTECTION OFFICERS

There is no legal requirement in Italy for organisations to appoint a data protection officer.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

As a general rule, processing of personal (non sensitive) data by private entities or profit seeking public bodies is only allowed if the data subject gives his/her express consent (Section 23 of the Privacy Code).

The data subject's consent is deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with a privacy information notice compliant with section 13 of the Privacy Code.

Nevertheless, pursuant to Section 24 of the Privacy Code, consent is not required if the processing of personal (non sensitive) data:

a) is necessary to comply with an obligation imposed by a law, regulations or EU legislation;

b) is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract;

c) concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and EU legislation with regard to their disclosure and publicity;

d) concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;

e) is necessary to safeguard life or bodily integrity of a third party. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted;

f) is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefore by complying with the legislation in force concerning business and industrial secrecy, dissemination of the data being ruled out;

g) is necessary to pursue a legitimate interest of either the data controller or a third party recipient in the cases specified by the Garante on the basis of the principles set out under the law, unless said interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests, dissemination of the data being ruled out;

h) except for external communication and dissemination, is carried out by non profit associations, bodies or organisations, recognised or not, with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice provided for by Section 13 of the Privacy Code;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

i) is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice referred to in Annex A) of the Privacy Code, or else exclusively for historical purposes in connection either with private archives that have been declared to be of considerable historical interest pursuant to Section 6(2) of legislative decree no. 499 of 29 October 1999, adopting the consolidated statute on cultural and environmental heritage, or with other private archives pursuant to the provisions made in the relevant codes;

j) concerns information contained in the CVs as per Section 13(5 bis) of the Privacy Code;

k) except for dissemination and subject to Section 130 hereof, concerns communication of data between companies, bodies and/or associations and parent, subsidiary and/or related companies pursuant to Section 2359 of the Civil Code, or between the former and jointly controlled companies, or between consortiums, corporate networks and/or corporate joint ventures and the respective members, for the administrative and accounting purposes specified in Section 34(1 ter) of the Privacy Code, providing such purposes are expressly referred to in a decision that shall be disclosed to data subjects jointly with the information notice referred to in Section 13 of the Privacy Code.

Sensitive data may only be processed with the data subject's written consent and the Garante's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations, unless:

a) the data concerns members of religious denominations and entities having regular contact with said denominations for exclusively religious purposes, on condition that the data are processed by the relevant organs or bodies recognised under civil law and are not communicated or disseminated outside said denominations. The latter shall lay down suitable safeguards with regard to the processing operations performed by complying with the relevant principles as set out in an authorisation by the Garante;

b) the data concerns affiliation of trade unions and/or trade associations or organisations to other trade unions and/or trade associations, organisations or confederations;

c) the data contained in CVs under the terms set forth in Section 13(5 bis) of the Privacy Code.

Sensitive data may also be processed without consent, subject to the Garante's authorisation:

- if the processing is carried out for specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements by not for profit associations, bodies or organisations, whether recognised or not, of political, philosophical, religious or trade unionist nature, including political parties and movements, with regard to personal data concerning members and/or entities having regular contacts with said associations, bodies or organisations in connection with the aforementioned purposes, provided that the data are not communicated or disclosed outside and the bodies, associations or organisations lay down suitable safeguards in respect of the processing operations performed by expressly setting out the arrangements for using the data through a resolution that shall be made known to data subjects at the time of providing the information under Section 13 of the Privacy Code;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- if the processing is necessary to protect a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted;
- if the processing is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor. Said claim must not be overridden by the data subject's claim, or else must consist in a personal right or another fundamental, inviolable right or freedom, if the data can disclose health and sex life; or
- if the processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also with regard to occupational and population hygiene and safety and to social security and assistance purposes, to the extent that it is provided for in the authorisation and subject to the requirements of the code of conduct and professional practice referred to in Section 111 of the Privacy Code.

The Garante has issued general authorizations for the processing of sensitive data.

TRANSFER

The data controller, may freely transfer personal data among the EU Member States. Such transfer can only be prohibited when it is made for the purposes of avoiding the measures that would be applied pursuant to the Privacy Code.

Personal data that is the subject of processing may be transferred from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever:

- if the data subject has given his/her consent either expressly or, where the transfer concerns sensitive data, in writing;
- if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject;
- if the transfer is necessary for safeguarding a substantial public interest that is referred to by laws or regulations, or else that is specified in pursuance of Sections 20 and 21 of the Privacy Code where the transfer concerns sensitive or judicial data;
- if the transfer is necessary to safeguard a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted;

- if the transfer is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are transferred exclusively for said purposes and for no longer than is necessary therefor in compliance with the legislation in force applying to business and industrial secrecy;
- if the transfer is carried out in response to a request for access to administrative records or for information contained in a publicly available register, list, record or document, in compliance with the provisions applying to this subject-matter;
- if the transfer is necessary, pursuant to the relevant codes of conduct referred to in Annex A) of the Privacy Code, exclusively for scientific or statistical purposes, or else exclusively for historical purposes, in connection with private archives that have been declared to be of considerable historical interest under Section 6(2) of legislative decree no. 490 of 29 October 1999, enacted to adopt the consolidated statute on cultural and environmental heritage, or else in connection with other private archives pursuant to the provisions made in said codes.

The transfer of processed personal data to a non-EU Member State shall also be permitted if it is authorised by the Garante on the basis of adequate safeguards for data subjects' rights:

- as determined by the Garante also in connection with contractual safeguards, or else by means of rules of conduct as in force within the framework of companies all belonging to the same group. A data subject may establish his/her rights in the State's territory as set forth by this Code also with regard to non compliance with the aforementioned safeguards; or
- as determined via the decisions referred to in Articles 25(6) and 26(4) of Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, through which the European Commission may find that a non EU Member State affords an adequate level of protection, or else that certain contractual clauses afford sufficient safeguards.

It is prohibited to transfer personal data that is the subject of processing from the State's territory to countries outside the European Union, temporarily or not and in any form and by any means whatsoever, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals.

Account shall also be taken of the methods used for the transfer and the envisaged processing operations, the relevant purposes, nature of the data and security measures.

SECURITY

Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B to the Privacy Code:

- computerised authentication;
- implementation of authentication credentials management procedures;
- use of an authorisation system;
- regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenance electronic means;
- protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software;
- implementation of procedures for safekeeping backup copies and restoring data and system availability;
- keeping an up to date security policy document (exceptions to this duty are provided for by the Privacy Code);
- implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

Processing personal data without electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B to the Privacy Code:

- regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of the processing and/or by the individual organisational departments;
- implementing procedures such as to ensure safekeeping of records and documents committed to the entities in charge of the processing for the latter to discharge the relevant tasks; or
- implementing procedures to keep certain records in restricted access filing systems and regulating access mechanisms with a view to enabling identification of the entities in charge of the processing.

Certain data controllers are allowed to implement simplified security measures.

BREACH NOTIFICATION

Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) amended the Privacy Code provisions in relation to breach notification by introducing (i) the definition of "personal data breach" (meaning "*a breach of security leading to the accidental destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service*" – Section 4, par. 3, let. g-*bis*) and (ii) new obligations in case of personal data breach.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

In particular, in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the Garante. When the personal data breach is likely to adversely affect the personal data or privacy of a contracting party or other individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification shall not be required if the provider has demonstrated that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. The notification to the contracting party or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the Garante shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach (Section 32-*bis* of the Privacy Code).

ENFORCEMENT

The Garante is authorised to investigate complaints and to impose sanctions. The Garante may also appoint experts, proceed with inspections, require to produce documents and to be granted access. In case of criminal actions, the Garante notifies the public prosecutor.

The Privacy Code provides for the following administrative sanctions:

- providing no or inadequate information to data subjects shall be punished by a fine consisting in payment of between six thousand and thirty six thousand Euro (Section 161 of the Privacy Code);
- processing personal data without the relevant data subject consent (if required) shall be punished by a fine consisting in payment of between ten thousand and one hundred and twenty thousand Euro (Section 162 of the Privacy Code);
- processing personal data without submitting the notification to the Privacy Commissioner (if required) shall be punished by a fine consisting in payment of between twenty thousand and one hundred and twenty thousand Euro (Section 163 of the Privacy Code).

Where any of the violations referred to in Sections 161, 162 and 163 is less serious by having also regard to the social and/or business features of the activities at issue, the upper and lower thresholds set forth in the said sections shall be reduced to two-fifths thereof (Section 164-*bis*, par. 1 of the Privacy Code).

Where one or more provisions mentioned above are violated repeatedly, also on different occasions, in connection with especially important and/or large databases, an administrative sanction shall be applied as consisting in payment of a fine ranging from fifty thousand and three hundred thousand Euro (Section 164-*bis*, par. 2 of the Privacy Code).

In other, more serious cases, in particular if the prejudicial effects produced on one or more data subjects are more substantial or if the violation concerns several data subjects, the upper and lower thresholds of the applicable fines shall be doubled (Section 164-*bis*, par. 3 of the Privacy Code).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The fines referred above may be increased by up to four times if they may prove ineffective on account of the offender's economic status (Section 164-*bis*, par. 4 of the Privacy Code).

The Privacy Code also provides for certain criminal sanctions.

ELECTRONIC MARKETING

The Privacy Code (Section 130) does not prohibit the use of personal data for the purpose of electronic marketing, but it requires the prior informed consent (*opt-in*) from the recipient of the communication. The use of automated calling or communications systems without human intervention for the purposes of direct marketing or for sending advertising materials, or else for carrying out market surveys or interactive business communication, as well as electronic communications performed by e-mail, facsimile, MMS or SMS-type messages, shall only be allowed with the contracting party's or user's consent.

Electronic marketing communications shall clearly identify the sender and provide to the recipient all necessary information in order for him/her to eventually refuse the delivery of the direct marketing material (*opt-out*).

The possibility for the recipient to opt-out from marketing communication services must be guaranteed both during the first contact with the recipient and during any following communications.

Marketing communications by way of non-automated telephone calls are permitted provided that either (i) the data subject has given his prior consent or (ii) the number of the data subject is included in the telephone directory and (s)he has not entered in a public opt-out register (*Registro delle Opposizioni*) and opted out from being contacted for marketing purposes.

Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) amended the Privacy Code provisions relating to marketing and commercial communications by making reference to the "contracting party's and user's consent" rather than to the "data subject's consent", given that the definition of "data subject" has been recently amended so as to include only natural persons and exclude companies from the application of the Privacy Code, with the exceptions of electronic marketing provisions. Indeed, the Garante clarified that the provisions of the Privacy Code on marketing obligations still apply to companies as well (and not only to natural persons).

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The Privacy Code as amended by Legislative Decree No. 69/2012 (implementing the Directive 2009/12/EC) regulates the collection and processing of traffic data and location data by the provider of a public communications network or publicly available electronic communications service and the use of cookies.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

According to Section 123 of the Privacy Code, traffic data shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication. However traffic data can be retained for a period not longer than 6 months for billing and interconnection payments purposes or, with the prior consent of the contracting party or user (which may be withdrawn at any time), for marketing electronic communications services or for the provision of value added services.

According to Section 126 of the Privacy Code, location data may only be processed if made anonymous or if the subscriber or user has been properly informed and (s)he has given her/his prior consent (which can be withdrawn at any time).

According to Section 122 of the Privacy Code (which reflects recital 66 of the E-Cookies Directive 2009/136/EC and the amended Section 5, par. 3 of the Directive 2002/58/EC – as amended by Directive 2009/136/EC) the storing of information in the contracting party's or user's computer is only allowed if said contracting party or user has been properly informed and (s)he has given her/his consent.

The Privacy Code states that the Garante may determine certain simplified modalities to provide contracting parties or users with the information notice and to identify the most efficient and practical ways to implement the new obligations on cookies. For this purpose, the Garante has recently launched a consultation with which it has also provided some FAQs that shed some light on the Garante's general view on cookies. The Garante confirmed its current trend to subject the cookies regulations to opt-in requirements, with limited exceptions, including analytics, authentication, flash players, "shopping baskets". To better assess the cookies issue under Italian Law, we therefore need to wait for the Garante's guidelines on cookies after the public consultation.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

29. JAPAN

CONTRIBUTION DETAILS

Lawrence G. Carter
Senior Associate
T +81 3 4550 2800
lawrence.carter@dlapiper.com

Ryo Takizawa
Associate
T +81 3 4550 2800
mizuho.miyata@dlapiper.com

LAW

The Act on the Protection of Personal Information ("**APPI**") requires business operators who utilize for their business in Japan a personal information database which consists of more than 5,000 individuals in total identified by personal information on any day in the past six months to protect personal information. In addition, various ministries, including the Ministry of Health, Labor and Welfare, the Japan Financial Services Agency and the Ministry of Economy, Trade and Industry have created guidelines regarding the APPI. These Guidelines are not laws, but are very persuasive in Japan and generally followed by business operators to which they apply.

DEFINITION OF PERSONAL DATA

Personal information is information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information. Personal Information includes information which enables one to identify specific individual with easy reference to other information.

Personal data is personal information constituting a Personal Information Database, which is systematically arranged in a way that specific personal information can be easily retrieved by a computer, etc.

DEFINITION OF SENSITIVE PERSONAL DATA

The APPI does not have a definition of Sensitive Information. However, the Japan Financial Services Agency's "Guidelines for Personal Information Protection in the Financial Field" ("**JFSA Guidelines**") defines information related to political opinion, religious belief (religion, thought, creed), participation in a labor union, race, ethnicity, family origin, legal domicile (*honsekichi*), medical care, sexual life and criminal record as sensitive information. The JFSA Guidelines prohibit collecting, using or providing to a third party, sensitive information unless an exception provided for in the JFSA Guidelines applies.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

There is no one single central data protection authority in Japan. The Consumer Affairs Agency is a central authority of the APPI in general.

The Minister of Health, Labor and Welfare as well as the minister with the jurisdiction over the business operations of the business operator are the competent ministers for employment related personal information. The minister with jurisdiction over the business operations of the business operator is a competent minister for the handling of personal information other than employment related personal information.

REGISTRATION

Japan does not have a central registration system.

DATA PROTECTION OFFICERS

There is no specific legal requirement to appoint a data protection officer. However, some guidelines provide that specific employees should be assigned to control personal data (e.g. Chief Privacy Officer).

COLLECTION AND PROCESSING

- Specifying the Purpose of Use

  When handling personal information, a business operator must specify to the fullest extent possible the purpose of use of the personal information ("**Purpose of Use**"). Once a business operator has specified the Purpose of Use, it must not then make any changes to the said purpose which could reasonably be considered to be beyond the scope of what is duly related to the original Purpose of Use. In addition, when handling personal information, a business operator shall not handle the information beyond the scope that is necessary for the achievement of the Purpose of Use without a prior consent of the individual. In other words, the use of the information must be consistent with the stated Purpose of Use.

- Public Announcement of the Purpose of Use

  The Purpose of Use must be made known to the individual when personal information is collected or promptly thereafter and this can be made by a public announcement (such as posting the purpose on the business operator's website). When personal information is obtained by way of a written contract or other document (including a record made in an electronic or magnetic format, or any other method not recognisable to human senses), the business operator must expressly state the Purpose of Use prior to the collection.

  A business operator must "publicly announce" or "expressly show the Purpose of Use" in a reasonable and appropriate way. According to the "Guidelines for the APPI Concerning Fields of Economy and Industry" issued by the Ministry of Economy, Trade and Industry ("**METI Guidelines**"), the most appropriate method for a website to publicly announce the Purpose of Use of information collected, is a one click access on the homepage.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

- Disclosing/Sharing Personal Data

Personal data may not be disclosed to a third party without the prior consent of the individual, unless permitted by the exceptions under the APPI. Even disclosing the data within group companies is considered disclosing the data to a third party and consent must be obtained.

The APPI does not provide any examples of how best to obtain consent from individuals before sharing information. Generally, written consent should be obtained whenever possible. When obtaining consent it would be prudent, to clearly disclose to the individual the identity of the third party to whom the personal data will be disclosed, the contents of the personal data and how the third party will use the provided personal data.

If personal data is to be used jointly, the business operator collecting the information could, prior to the joint use, notify the individuals providing the personal information of the following: the fact that the personal data will be used jointly, the items of the personal data used jointly, the scope of the joint users, the purpose for which the personal data will be used by them and the name of the individual or business operator responsible for the management of the personal data.

- Consents

The METI Guidelines provide the following examples as appropriate methods of obtaining the consent for disclosing personal data from the individual:

- receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from such person;
- receipt of a consent email from such person;
- the person's check of the confirmation box concerning the consents;
- the person's click of a button on the website concerning the consents; and
- the person's audio input, or touch of a touch panel concerning the consents.

- Supervision of Trustees

When a business operator entrusts an individual or another business operator with the handling of personal data in whole or in part, it must exercise all necessary and appropriate supervision over the trustee to ensure that the use of the entrusted personal data is securely controlled.

Providing a trustee with personal data under these circumstances is not considered to be disclosing personal data to a third party under the APPI.

Even if this exception does apply, it should be noted that a business operator which entrusts a third party with the handling of personal data has a statutory obligation of supervision over the trustee.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

The APPI requires that business operators prevent the leakage of personal data. The APPI does not set forth specific steps that must be taken. Ministry guidelines impose specific steps that business operators should take to ensure that personal data is secure. These necessary and appropriate measures generally include "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures".

Guidelines often contain several specific steps or examples that entities subject to the Guidelines must take with respect to each of the security control measures such as developing internal guidelines pertaining to security measures, executing non-disclosure contracts with employees who have access to personal data, protecting machines and devices and developing a framework to respond to instances of leakage.

BREACH NOTIFICATION

The APPI does not explicitly require notification to a ministry or governmental authority in the event of a leak or security breach that may lead to a leak of personal data, although a ministry may request that a report be submitted.

However, the JFSA Guidelines provide that a business operator regulated by the JFSA must immediately produce a report when a leakage of personal information occurs. In addition, the business operator must promptly publicise the facts related to the leakage and the steps taken to prevent the reoccurrence of similar event. Finally, the JFSA Guidelines require that the business operator notify the individual whose information has been leaked of the leakage.

The METI Guidelines provide suggested measures that business operators, subject to the Guidelines, should take if there is a leak or breach of security with respect to personal data.

The METI Guidelines' measures include the following: (i) a business operator should notify the individuals whose personal data may have been compromised, although there may be circumstances where notifying individuals may not be necessary depending on the specific facts. Relevant factors to consider are the harm (including potential harm) to the individuals concerned; (ii) a business operator should voluntarily file a report of the incident with METI. METI will potentially make such reports public; and (iii) a business operator should make public the nature of the incident, the steps taken to ensure that it does not happen again.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

Enforcement of the APPI is handled by the minister with jurisdiction over the business of the business operator; and Minister of Health, Labor and Welfare with respect to the employment.

The minister may:

- require an business operator to submit reports regarding the handling of personal information;
- provide necessary advice to the business operator with respect to the entity's handling of personal information;
- recommend an business operator to cease violations or correct violations of the specific provisions of the APPI; and
- order an business operator to take the recommended or necessary measures.

If the business operator does not provide a report as required by a minister or has made a false report the business operator is subject to a fine of up to JPY300,000. If the business operator fails to follow a corrective order by a minister, the business operator is subject to a fine of up to JPY300,000 or imprisonment with work of up to six months. In addition, the entity shall be sentenced to the fine if an officer or an employee of the entity commits any of the above violation concerning the business of the entity.

ELECTRONIC MARKETING

The Act on Specified Commercial Transactions ("ASCT") and the Act on the Regulation of Transmission of Specified Electronic Mail ("Anti-Spam Act") regulate the sending of unsolicited electronic commercial communications.

Under the ASCT, which focuses on internet-order services and mail-order services, a seller is prohibited from sending email advertisements to consumers unless they provide a prior request or consent (i.e. an opt-in requirement). The seller is also required to retain the records that show consumers' requests or consents to receive email advertisements for 3 years after the last transmission date of an email advertisement to the consumer.

If a seller has breached any of these obligations, such seller will be potentially subject to fine of up to JPY 1,000,000.

Under the Anti-Spam Act, which broadly covers commercial emails (e.g. an invitation email from a social network service), there are several regulations on sending email advertisements as follows:

- The sender must retain records evidencing there was a request or consent to receive emails at least for 1 month after the last date the seller sent an email to the recipient.
- For-profit entities or individuals engaged in business sending any email to advertise their own or another's business must obtain a request or consent to receive emails from intended recipients unless the recipient falls under certain exceptions (e.g. there is a continuous transaction relationship between a sender and a recipient) in the Anti-Spam Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- An email is required to include a sender's email address or a URL so that recipients can send opt-out notices to the sender.
- Senders must not send emails to randomly generated email addresses (with the hope of hitting an actual email address) for the purpose of sending emails to a large number of recipients.

The relevant ministry may order a sender to improve the manner of email distribution if the sender violates the requirements noted above. If the sender violates an order issued by the ministry (other than one related to the retention obligation), the sender is subject to imprisonment for up to 1 year or a fine of up to JPY 1,000,000. The entity will be subject to fine of up to JPY 30,000,000 if an officer or an employee of the entity commits any violation mentioned above. If the sender violates an order issued by the minister with respect to the retention obligation, the sender will be potentially subject to fine of up to JPY 1,000,000.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no law in Japan that specifically addresses cookies and location data. However, if the information obtained through cookies may identify a certain individual in conjunction with other easily-referenced information (e.g. member registration) and it is utilised (e.g. for marketing purposes), such Purpose of Use of information obtained through the use of cookies must be disclosed under the APPI. METI takes the same position in its guidelines.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

30. LITHUANIA

CONTRIBUTION DETAILS

LAWIN

www.lawin.com

Prof. Dr. Mindaugas Kiškis
Associate Partner
T +370 5 2681815
M +370 5 2681888
mindaugas.kiskis@lawin.lt

LAW

As a member of the European Union, Lithuania has implemented the EU Data Protection Directive 95/46/EC which is step by step amending its national legislation. Lithuania passed the Law on Legal Protection of Personal Data on 11 June 1996 (the "**Data Protection Law**"), which has been amended on 17 July 2000, 22 January 2002 and 21 January 2003 in order to transpose the provisions from the Directive. The latest modifications to the Data Protection Law came into force on 1 September 2011. They include amendments and new regulations on public polls, credit referencing agencies and public governance of data protection. Enforcement is carried out by the State Data Protection Inspectorate.

In addition, Lithuania has fully transposed the Directive 2006/24/EC (the Data Retention Directive) into national law through the Law on Electronic Communications dated 15 April 2004 (latest amendments came into force on 1 August 2011). The Law on Electronic Communications governs protection of privacy in the area of electronic communications.

DEFINITION OF PERSONAL DATA

Any information relating to a natural person, the data subject, who is identified or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

DEFINITION OF SENSITIVE PERSONAL DATA

Data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sex life and criminal convictions.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The State Data Protection Inspectorate (the "**Inspectorate**").

A. Juozapavičiaus str. 6/Slucko str. 2
LT-09310 Vilnius
Lithuania
T +370 5 279 1445
F +370 5 261 9494
ada@ada.lt
www.ada.lt

The Inspectorate's mission is to ensure high level of data protection. The Inspectorate tries to ensure that data controllers and providers of public communications networks and publicly available electronic communications services fulfil the requirements set up for data protection.

REGISTRATION

Only data controllers who process data by automatic means are obliged to undergo mandatory registration. The Data Protection Law establishes the requirement, that such data processing may be carried out only when the data controller or his representative notifies the Inspectorate except cases where personal data is processed:

- for the purposes of internal administration (including group level administration);
- for political, philosophical, religious or trade union related purposes by a foundation, association or any other non profit organisation on the condition that the personal data processed relates solely to the members of such organisation or to other persons who regularly participate in its activities in connection with the purposes of such organisations;
- by the media for the purpose of providing information to the public for artistic and literary expression; or
- in accordance with regulation on state secrets and official secrets.

The data controller when notifying the Inspectorate of data processing has to submit a standard notification form, which includes information about:

- the purpose of the data processing;
- the groups of data subjects;
- the sources of the personal data;
- the groups of the receivers of the data;
- the list of categories of personal data that are being processed;
- the personal data transfers to foreign countries;
- the personal data retention period;
- the data processors; and
- the list of security measures.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

After notification, data controllers are registered in the State Register of Personal Data Controllers which is administered by the Inspectorate. The notification and registration of data controllers is free of charge.

If data is not processed by automatic means, there is no obligation to notify the Inspectorate. However, certain data processing may be carried out only if an authorisation has been granted by the Inspectorate after prior checking of the data processing. The Inspectorate shall carry out prior checking of personal data processing in the following cases:

- where the data controller intends to process sensitive personal data by automatic means, except where the processing is carried out for the purposes of internal administration or in the cases of prevention and investigation of criminal or other illegal activities, as well as court hearings;
- where the data controller intends to process public data files by automatic means, unless laws and other legal acts lay down a procedure for the disclosure of data;
- where the data controller of state or institutional registers or information systems of state and municipal institutions intends to authorise the data processor to process personal data, except in cases where laws and other legal acts establish the right of the data controller to authorise a particular data processor to process personal data or where the data processor is a legal person established by the data controller;
- health data is being processed by automatic means or for scientific medical research purposes;
- data is being processed in relation to evaluating a person's solvency and managing his/her debt; or
- data is being processed for statistical, historical or scientific research purposes.

DATA PROTECTION OFFICERS

Under the legislation of Lithuania the organisations (data controllers) have a right (but not an obligation) to designate a person to be responsible for the data protection ("Data Protection Officer"). The data controller must notify the Inspectorate of appointment or withdrawal of the data protection officer within 30 days.

The data protection officer shall:

- make public the processing of personal data actions carried out by the data controller in accordance with the procedure established by the Government;
- supervise as to whether personal data is processed in compliance with the provisions of the Data Protection Law and other legal acts on data protection;
- initiate the preparation of the notifications to the Inspectorate in case of prior checking;
- monitor the processing of personal data carried out by the data controller's employees;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- present proposals, findings to the data controller regarding establishment of data protection and data processing measures and supervise implementation and use of these measures;
- undertake measures to eliminate any violations in the processing of personal data without delay;
- instruct employees authorised to process personal data on the provisions of Data Protection Law and other legal acts on personal data protection;
- initiate the preparation of applications to the Inspectorate of the inquiries regarding processing and protection of personal data;
- assist data subjects in exercising their rights; and
- notify the Inspectorate in writing where the data controller processes personal data in violation of the data protection laws and refuses to rectify these violations.

In addition, if no data protection officer is appointed, the CEO of the data controller will be ex officio deemed responsible for data protection compliance and will be also personally liable for any legal violations of the Data Protection Law.

COLLECTION AND PROCESSING

The term data processing means any operation, which is performed in relation to personal data (eg collection, recording, storage, classification combining, disclosure, making available, use, destruction or etc.). It must be carried out in accordance with the requirements and in cases set by laws. According to the Data Protection Law personal data may be processed if:

- the data subject has given his consent;
- a contract to which the data subject is party is being concluded or performed;
- it is a legal obligation of the data controller under laws to process personal data;
- processing is necessary in order to protect vital interests of the data subject;
- processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data are disclosed;
- processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data is disclosed, unless such interests are overridden by interests of the data subject.

Sensitive personal data (data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life and criminal convictions) can only be processed in the following cases:

- the data subject has given his consent (ie expressed clearly, in a written or equivalent form or any other form giving unambiguous evidence of the data subject's free will);

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- such processing is necessary for the purposes of employment or civil service while exercising rights and fulfilling obligations of the data controller in the field of labour law in the cases laid down in law;
- it is necessary to protect the vital interests of the data subject or of any other person, where the data subject is unable to give his consent due to a physical disability or legal incapacity;
- the processing of personal data is carried out for political, philosophical, religious purposes or purposes concerning the trade unions by a foundation, association or any other non profit organisation, as part of its activities, on condition that the personal data processed concern solely the members of such organisation or to other persons who regularly participate in such organisation in connection with its purposes;
- the personal data has been made public by the data subject;
- the data is necessary, in the cases laid down in law, in order to prevent and investigate criminal or other illegal activities;
- the data is necessary for a court hearing; or
- it is a legal obligation of the data controller under laws to process such data.

In addition, it must be mentioned that the data controller must provide the fair processing information to data subjects in cases where personal data has been obtained directly or from a third party or prior to it being released to a third party, except where the data subject already has it. It shall contain information about:

- the identity and permanent place of residence of himself (the data controller) and his representative, if any (where the data controller or his representative is a natural person), or requisites and the address of registered office (where the data controller or its representative is a legal person);
- the purposes of the processing of the data subject's personal data;
- other additional information (the recipient and the purposes of disclosure of the data subject's personal data; particular personal data that the data subject must provide and the consequences of his failure to provide the data, the right of the data subject to have an access to his personal data and the right to request the rectification of incorrect, incomplete and inaccurate personal data) to the extent that is necessary for ensuring fair processing of personal data without infringing upon the data subject's rights.

TRANSFER

All cross border transfers of personal data within the European Economic Area (the European Union countries plus Norway, Liechtenstein and Iceland) shall take place on the same conditions and in accordance with the same procedure applicable to data recipients in Lithuania. Cross-border transfers outside the European Economic Area shall be subject to special authorization from the Inspectorate unless the exceptional conditions for cross border data transfer are satisfied. These are cases where:

- the data subject has given his consent for the transfer of his personal data;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the transfer of personal data is necessary for the conclusion or performance of a contract between the data controller and a third party in the interests of the data subject;
- the transfer of personal data is necessary for the performance of a contract between the data controller and the data subject or for the implementation of pre contractual measures to be taken in response to the data subject's request;
- the transfer of personal data is necessary (or required by law) for important public interests or for the purpose of legal proceedings;
- the transfer is necessary for the protection of vital interests of the data subject;
- the transfer is necessary for the prevention or investigation of criminal offences;
- personal data is transferred from a public data file in accordance with the procedure laid down in law and other legal acts.

The Inspectorate shall grant authorization provided that an adequate level of legal protection of personal data is ensured in the recipient's country or by the means of transferring (i.e. adequate data protection safeguards). In practice adequate level of protection may be achieved by the following means:

- model contractual clauses approved by the European Commission;
- Binding Corporate Rules;
- personal data is transferred to countries whitelisted by the European Commission; or
- personal data transfers to the United States companies, which have subscribed to the Safe Harbour principles.

SECURITY

Lithuanian data protection legislation obliges the data controller and data processor to implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing. Moreover, they must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.) in accordance with the general requirements on the organisational and technical data protection measures laid down by the Inspectorate. Key measures taken shall be disclosed to the Inspectorate through the data controller registration form.

BREACH NOTIFICATION

The providers of publicly available electronic communications services have the obligation to notify the personal data breach to the Inspectorate without undue delay. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider must also notify the subscriber or individual of the breach, except where the provider

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

has demonstrated to the satisfaction of the Inspectorate that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the Inspectorate, having considered the likely adverse effects of the breach, may require it to do so.

Other data controllers do not possess a general obligation to notify individuals or the Inspectorate of a data security breach. It may only be advisable as a part of bona fide obligations for minimising civil liability.

ENFORCEMENT

The implementation of the Data Protection Law shall be supervised and monitored by the Inspectorate. The key objectives of the Inspectorate shall be supervision of data controllers' activities when processing personal data, monitoring the legality of personal data processing, prevention of violations in data processing and ensuring protection of the rights of the data subject.

Any violation of data protection rules or breach of the rights of data subject causes administrative liability. No criminal liability is provided for data protection violations. The Inspectorate has no power to impose penalties for violations, although the Inspectorate can issue a statement on an administrative offence according to which national courts can impose fines from LTL 500 (approx. EUR 140) to LTL 2000 (approx. EUR 570). It shall be noticed that these administrative sanctions may only be applied to individuals and legal entities/companies may not be subject to administrative prosecution. If a company commits a violation, the Data Protection Officer or the CEO of the entity will be held responsible for such an administrative offence.

In addition, the individual affected by the breach of the Data Protection Law is also entitled to claim pecuniary and moral damages.

ELECTRONIC MARKETING

The Data Protection Law will apply to most electronic marketing activities, with the exception of e-mail marketing (which is regulated by the Law on Electronic Communications), as there is processing and use of personal data involved (e.g. an email address is deemed "personal data" for the purposes of the Data Protection Law). The rules set forth in both laws are generally identical.

The Data Protection Law does not prohibit the use of personal data for the purposes of electronic marketing but requires individuals to consent to the processing of their personal data for direct marketing purposes in advance (eg a right to "opt-in").

There is one exception from opt-in requirement, providing instead for an opt-out scheme.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Unsolicited electronic marketing, including emails, can only be sent without consent if:

- The contact detail have been provided in the course of a sale and the data subject is an existing customer;
- The marketing relates to a similar product;
- The recipient was given a means of refusing the use of their contact details for marketing when they were collected; and
- The recipient did not object to the direct marketing use at the time when his personal data was collected.

Direct marketing communication must not disguise or conceal the identity of the sender. SMS marketing is included within the regulations applicable to all direct marketing.

The above opt-out exception to existing customer applies in relation to individuals. For e-mail marketing opt-in is required from both individuals and corporations (all e-mail account holders without any exceptions). Otherwise for non-email electronic marketing only individual opt-in is required, and said existing client opt-out exception is allowed, if all of the conditions for this exception are fulfilled.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The PEC Regulations (as amended by Directive 2009/12/EC) are implemented in Lithuania through the Law on Electronic Communications. Amendments of the Law on Electronic Communications which came into effect on 1 August 2011, implemented the Directive 2009/12/EC. Specifically the Law on Electronic Communications contains regulations on collection of location and traffic data by public electronic communications services providers ("**CSPs**") and use of cookies (and similar technologies).

Traffic Data – Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service;
- Consent has been given for the retention of the Traffic Data; and
- It is required for investigation of a grave crime.

Traffic Data can only be processed by a CSP for:

- The management of business needs, such as billing or traffic;
- Dealing with customer enquiries;
- The prevention of fraud; or
- The provision of a value added service.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Location Data – Location Data may only be processed for the provision of value added service with consent.

CSPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Cookie Compliance – The use and storage of cookies and similar technologies requires: a) clear and comprehensive information; and b) consent of the website user.

Lithuanian State Data Protection Inspectorate has published recommendations about the method of consent to the use for cookies. The guidance confirmed that consent can be obtained through pop-ups, banners or website registration while relevant settings contained within current browsers are not likely to form a valid consent. According to the guidance, the users must be given a genuine opportunity not to consent. There is no clear guidance on possibility to obtain an implied consent.

Consent is not required for cookies that are;

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

Enforcement of a breach of the PEC Regulations is dealt with by the Inspectorate and sanctions for breach are the same as set out in the Enforcement section above.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

31. LUXEMBOURG

CONTRIBUTION DETAILS

Bonn & Schmitt
22-24, Rives de Clausen
L-2165 Luxembourg
T +352 27 855
F +352 27 855 855
www.bonnschmitt.net

Alex Schmitt
Partner
T +352 27 855
aschmitt@bonnschmitt.net

Guy Arendt
Partner
T +352 27 855
garendt@bonnschmitt.net

Alain Grosjean
Partner
T +352 27 855
agrosjean@bonnschmitt.net

LAW

The law dated 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data as modified ("**Law**").

The Law dated 30 May 2005 lays down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector.

DEFINITION OF PERSONAL DATA

The Law defines "personal data" as follows: any information of any type regardless of the type of medium, including sound and image, relating to an identified or identifiable natural person ("**data subject**"); a natural person will be considered to be identifiable if it can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to its physical, physiological, genetic, mental, cultural, social or economic, identity."

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive data relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the health or sex life, including the processing of genetic data.

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale pour la Protection des Données ("**CNPD**")
41, avenue de la Gare
L-1611 Luxembourg 4ième étage
T +352 26 10 60 1
F +352 26 10 60 29

The CNPD is responsible for overseeing the Data Protection Act and the Privacy and Electronic Communications Regulations.

REGISTRATION

PRIOR NOTIFICATION TO THE CNPD

As the processing of personal data is not exempt from notification and is not subject to prior authorisation, it must be notified to the CNPD in advance. The notifications must contain the information referred to in Article 13 of the Law.

The notifications are effected by completing and signing the notification form provided by the CNPD. Article 13 of the Law provides 14 specific cases of conditional exemption from the obligation to notify which are added to the more general cases referred to in Article 12 § 2.

The most important exceptions relate to the following processing:

General exemptions (Art. 12 § 2)

- processing carried out by the controller if that person appoints a data protection officer unless for the supervision purposes referred to in Article 10 ("DPO");
- processing operations for the sole purpose of keeping a public register;
- processing operations carried out by lawyers, notaries and process servers;
- processing carried out solely by journalists, for artistic or literary expression; or
- processing necessary to protect the vital interests of the data subject or of another where the data subject is physically or legally incapable of giving his consent.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Conditional exemptions

- processing of data relating exclusively to personal data necessary for the administration of the salaries of persons in the service of or working for the controller;
- processing of data relating exclusively to the management of applications and recruitment, provided that the collected data is not sensitive data (including health) or data intended for assessing the data subject;
- processing of data relating exclusively to the controller's bookkeeping provided that this data is used exclusively for such bookkeeping and the processing covers only the persons whose data is necessary for bookkeeping purposes;
- processing of data referring exclusively to the administration of shareholders, debenture holders and partners, provided that the processing covers solely the data necessary for such administration, the data covers only those persons whose data is necessary for such administration;
- processing of data relating exclusively to the management of the controller's client or supplier base, provided that the processed data is not sensitive data (including health);
- processing of data carried out by a foundation, an association or any other non profit organisation;
- processing of data relating exclusively to the recording of visitors carried out in the context of manual access control, provided that the data processed is restricted to only the name and business address of the visitor, his/her employer, his/her vehicle, the name, department and function of the person visited, and the time and date of the visit;
- processing of identification data essential for communication, which is carried out with the sole purpose of contacting the person concerned provided that this data is not communicated to any other third party;
- processing for the management of IT systems, provided that it is not used for the purpose of supervision;
- processing carried out in hospitals or by a doctor concerning his/her patient, except for the processing of genetic data; or
- processing carried out by a pharmacist.

The Law has also reduced the procedures concerning processing in the health professions. Except for the processing of genetic data, there is no more requirement of prior authorisation concerning such a processing, and doctors and hospitals are exempt to the obligation to notify.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Prior authorisation by the CNPD

Most processing of personal data must only be notified (or is exempt from notification). However, the Law provides for stricter control for processing likely to present specific risks in respect of the rights and freedoms of individuals concerned. Such processing must be authorised by the CNPD before it may be carried out. The amended Law contains a closed list of these categories of processing in Article 14.

Article 14 1 of the Law sets forth that the prior authorisation by the CNPD is required in the following cases:

- the processing of genetic data;
- when processing is recorded and carried out for supervision purposes;
- when data is processed for statistic, scientific or historic purposes;
- in the event of the combination of data;
- when the processing relates to the credit status and solvency of the data subjects, if the processing is carried out by persons other than professionals of the financial sector or by insurance companies regarding their clients;
- processing involving biometric data necessary for checking personal identity; or
- the usage of data for purposes other than that for which it was collected. Such processing may be carried out only when the data subject gives prior consent or if it is necessary to protect the vital interests of the data subject.

Processing operations that reveal race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life, except for certain processing of genetic data, may only be notified to the CNPD and may not be authorised by the CNPD.

The processing of genetic data may only be notified to the CNPD when the processing is necessary to protect vital interests or when it is necessary for the purpose of preventive medicine, medical diagnostics, or the provision of care or treatment.

An authorisation from the CNPD is normally required before using technical means for monitoring people, particularly by video camera, electronic tracing, etc. However, the Law has introduced a distinction according to if the data is recorded or not recorded. The prior authorisation by the CNPD is required for processing for supervision purposes, if the data resulting from the supervision is recorded. A simple notification is required if the data resulting from the supervision is not recorded.

For the processing of credit status and solvency of the data subject, a simple notification is required, if the processing is carried out by professionals in the financial sector or insurance companies on behalf of their clients.

The processing of biometric data is subject to prior authorisation.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DATA PROTECTION OFFICERS

The controller may designate a DPO. Such designation releases the controller from the obligation to carry out the notifying process. Such a designation does not exempt the person responsible for processing from entering prior requests for authorisation before carrying out processing for which authorisation is required.

The power of the data protection official are as follows:

- investigative powers to ensure supervision of the controller's compliance with the provisions of the Law and its implementing regulations, and
- a right to be informed by the controller and the relating right to inform the controller of the formalities to be carried out in order to comply with the provisions of the Law and its implementing regulations.

COLLECTION AND PROCESSING

Chapter 2 of the Law deals with the conditions under which processing may take place. The controller must ensure that he processes the data in a fair and lawful manner, which means that:

- data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes;
- the collection, recording and use of personal data is strictly limited to what is necessary to achieve the aims specifically declared in advance by the authority, agency, company, association, professional or self employed worker involved;
- processing must be adequate and not excessive in relation to the purposes for which they are collected and/or further processed;
- the processing of personal data is limited to cases where there is a direct connection with the initial purpose of the processing. The information must not only be useful, but also necessary to whoever is processing personal data. The data being processed must not be excessive in relation to the aim pursued;
- an update of the collected data must be made;
- as inaccurate or incomplete information can harm the person to whom it relates, every effort must be made to ensure the data being processed is correct and up to date. If this is not the case, the personal data must be rectified or erased. The Law also protects the data subject against any negative decision automatically made about him by a computer, without him being able to provide his personal point of view; and
- data which permits identification of data subjects is only kept for the necessary period of time.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Legitimacy of processing

The processing of personal data is allowed only if there is a legitimate reason to justify it. Article 5 of the Law sets forth the criteria for the legitimacy of data processing, which is as follows:

Data may be processed only if it is necessary:

- for compliance with a legal obligation which the controller is subject to;
- for the performance of a task carried out in the public interest;
- for the performance of a contract to which the data subject is a party;
- for the purpose of legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interest, fundamental rights and/or freedoms of the data subject; or
- in order to protect the vital interests of the data subject.

Finally, the data processing is legitimate if the data subject has given his consent.

Processing of specific categories of data

Processing operations that reveal racial or ethnic origin, politic opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life, including the processing of genetic data, are forbidden and may only be allowed under very exceptional circumstances. Processing of specific categories of data by health services is strictly regulated. Legal data and freedom of expression are also strictly regulated.

Processing for supervision purposes

Article 10 sets out the conditions under which processing for supervision purposes in any place accessible or inaccessible to the public can be made. Processing for supervision purposes is considered legitimate in and around any place presenting a risk where it is necessary not only for the safety of users and the prevention of accidents, but also for the protection of property if there is a risk of theft or vandalism. The criteria of necessity and proportionality will be assessed for each individual case by the CNPD.

Article 10 1 of the Law sets forth that "the data may only be processed for supervision purposes:

- if the data subject has given his consent; or
- in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question due to its nature, position, configuration or frequentation presents a risk that makes the processing necessary for the safety of users and for the prevention of accidents, for the protection of property, if there is a characteristic risk of theft or vandalism; or
- in private places where the resident natural or legal person is the controller; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- to the competent legal authorities to record a criminal offence or take legal action in respect of it and to the legal authorities before which a legal right is being exercised or defended".

Processing for the purposes of supervision at the workplace

The supervision at the workplace is only possible under certain circumstances. Article 11 of the Law refers to Article L.261 1 of the Employment Code. Such processing may be carried out only if it is necessary:

- for the safety and health of employees;
- to protect the company's property;
- to control the production process relating solely to machinery;
- temporarily control production or the employee's services if such a measure is the only way of determining the exact earnings; or
- in connection with the organisation of work under a flexible hours scheme in accordance with the Employment Code.

The person whose data is processed must be informed prior to processing. The data subjects' consent to the processing does not, however, render the processing legitimate.

TRANSFER

Article 18 of the Law provides that data may be transferred to a third country, if this country ensures an adequate level of protection and if the provisions of the Luxembourg Law on data protection as well as its regulations are respected. The adequacy of the level of protection afforded by a third country must be assessed by the controller in light of all circumstances surrounding a data transfer operation or set of data transfer operations; particularly, the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectored, in force in the third country in question and the professional rules and security measures which are complied with by that country. In case of any doubt, the controller will immediately inform the CNPD which will consider whether the third country offers an adequate level of protection.

The transfer of data to a third country that does not offer an adequate level of protection may take place provided:

- the data subject has given his consent to the proposed transfer;
- the transfer is necessary for the performance of a contract to which the data subject and the controller are parties, or the implementation of pre contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or to establish, exercise or defend a legal claim; or
- the transfer is necessary for a public register.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The CNPD may authorise, as a result of a duly reasoned request, a transfer of data to a third country that does not provide an adequate level protection, if the controller offers sufficient guarantees in respect of the protection of the privacy, freedoms and fundamental rights of the data subjects, as well as the exercise of any corresponding rights. These guarantees may result from appropriate contractual clauses.

SECURITY

The controller must implement all appropriate technical and organisational measures to ensure the protection of the data he processes against accidental or unlawful destruction or accidental loss, falsification, unauthorised dissemination or access in particularly where the processing involves the transmission of data over a network, and against all other unlawful forms of procession. The initial Law sets forth these measures had to be contained in an annual report to be submitted by the controller to the CNPD. The 2007 Law has amended this automatic obligation. Article 22 of the Law provides that "a description of these measures and of any subsequent major change must be communicated to the CNPD at its request, within fifteen days".

If the processing is carried out on behalf of the controller, the latter must choose a processor that provides sufficient guarantees as regards the technical and organisational security measures. Any processing carried out on another's behalf must be governed by a written contract binding the processor to the controller and providing in particular that the processor will act only on instructions from the controller and the obligations relating to security of processing operations will be also incumbent on the processor.

BREACH NOTIFICATION

Any party that does not carry out the obligation to notify or supplies incomplete or inaccurate information is liable to a fine of between EUR 251 and EUR 125,000.

BREACH AUTHORISATION

Any party who carries out processing in breach of obtaining a prior authorisation will be liable to a prison sentence of between 8 days and 1 year and a fine between EUR 251 to EUR 125,000.

ENFORCEMENT

Without prejudice to criminal sanctions provided for by the Law, and any actions for damages under ordinary civil law, in the event a processing operation violates formalities provided for under Law, the State Prosecutor, the CNPD or any injured party is entitled to file a discontinuance action pursuant to Article 39 of the Law.

ELECTRONIC MARKETING

Luxembourg implemented part of Directive 2009/136/EC by a law of 28 July 2011, which modified the law of 30 May 2005 and came into effect on 1 September 2011.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is permissible only in respect of subscribers who have given their prior consent.

Where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in the previous paragraphs shall be permissible only with the prior consent of the subscriber concerned.

Online PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Traffic Data – For the purposes of the investigation, detection and prosecution of criminal offences, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing traffic data must retain such data for a period of 6 months. This obligation includes data related to the missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase these data unless such data have been made anonymous.

Traffic data may be processed for the purposes of marketing electronic communications services or providing value added services, to the extent and for the duration necessary for such supply or marketing of such services, provided that the provider of an electronic communications service or the operator has informed the subscriber or user concerned in advance of the types of traffic data processed and of the purpose and duration of the processing, and provided that the subscriber or user has given his/her consent, notwithstanding his/her right to object to such processing at any time.

Location Data other than Traffic Data – Service providers or operators have also an obligation of retaining location data other than traffic data for a period of 6 months for the purposes of the investigation, detection and prosecution of criminal offences. This obligation includes data related to the missed phone calls wherever these data are generated, stored or recorded. Beyond this period, the service provider or operator must erase these data unless such data have been made anonymous.

Service providers or operators may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or the subscriber or user concerned has given his/her consent thereto, to the extent and for the duration necessary for the supply of a value added service.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Service providers and, where appropriate, operators shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the value added service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time.

Where consent of the subscribers or users has been obtained for the processing of location data other than traffic data, the subscriber or user must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Cookies – Prior informed consent of a subscriber/user is required. The method of providing information and the right to refuse should be as user friendly as possible and, where it is technically possible and effective, the users consent may be expressed by appropriate browser/application settings.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

32. MALAYSIA

CONTRIBUTION DETAILS

Zaid Ibrahim & Co
Level 19 Menara Milenium
Pusat Bandar Damansara
50490 Kuala Lumpur
http://www.zicolaw.com

Sharon Tan
Partner
T +603 20879849

LAW

At present, Malaysia does not have any comprehensive data protection law in force. In the absence of an overarching protection of personal information, obligations of secrecy have been imposed in a piecemeal manner by statute or industry codes in specific circumstances. Confidentiality of information is usually protected using contractual obligations or the common law of confidence.

However, this situation will soon change. Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 ("**PDPA**"), has been passed by the Malaysian Parliament. However, at the time of writing, no date has been set for the PDPA to come into force.

DEFINITION OF PERSONAL DATA

"**Personal data**" means any information in respect of commercial transactions, which:

- is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

"**Sensitive personal data**" means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister of Information, Communications and Culture ("**Minister**") may determine by order published in the *Gazette*.

NATIONAL DATA PROTECTION AUTHORITY

Currently, there is no centralised data protection authority in Malaysia.

Pursuant to the PDPA, a Personal Data Protection Commissioner ("**Commissioner**") will be appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee. Decisions of the Commissioner can be appealed against through the Personal Data Protection Appeal Tribunal.

REGISTRATION

Currently, there is no centralised data protection authority in Malaysia.

When the PDPA comes into operation, the Minister may specify a class of data users who shall be required to be registered as data users.

DATA PROTECTION OFFICERS

Currently, there is no requirement for data users to appoint a data protection officer in Malaysia. There is also no such requirement under the PDPA.

COLLECTION AND PROCESSING

Currently, there are no specific legislative requirements for the collection and processing of personal data in Malaysia.

Under the PDPA, subject to certain exceptions, data users are generally required to obtain the consent of data subjects for the processing (which includes collection and disclosure) of their personal data. There are also other obligations imposed on the data user in relation to the processing of personal data, including, for example, requirements to notify the data subjects regarding the purpose for which their personal data are collected.

TRANSFER

Currently, there are no specific legislative requirements for the transfer of personal data in Malaysia.

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

However, there are exceptions to this restriction, such as where:

- the data subject has given his consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data user;
- the data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner which, if that place were Malaysia, would contravene the PDPA; and
- the transfer is necessary to protect the data subject's vital interests.

SECURITY

Currently, there are no specific legislative requirements for the imposition of security measures for the protection of personal data in Malaysia.

Under the PDPA, data users have an obligation to take "practical" steps to protect personal data.

BREACH NOTIFICATION

Currently, there are no specific legislative requirements for data users to notify authorities regarding data protection breaches in Malaysia.

The PDPA is also silent on this issue.

ENFORCEMENT

Currently, there are no specific legislative provisions for the enforcement of personal data protection in Malaysia.

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA.

Violation of the PDPA attracts criminal liability. The prescribed penalties include the imposition of fines or a term of imprisonment or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defence.

However, there is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing. "Direct marketing" means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

LINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, when the PDPA comes into force, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

33. MALTA

CONTRIBUTION DETAILS

Mamo TCV Advocates
Palazzo Pietro Stiges
90 Strait Street
Valletta VLT 1436
Malta
T +356 21 231 345
info@mamotcv.com
www.mamotcv.com

Dr. Antoine Camilleri
Partner
antoine.camilleri@mamotcv.com

Dr. Claude Micallef-Grimaud
Associate
claude.micallefgrimaud@mamotcv.com

LAW

The relevant law is the Data Protection Act ("**Act**") (Chapter 440 of the Laws of Malta) and the Regulations (at present six in number) issued under it.

DEFINITION OF PERSONAL DATA

Personal data is defined in the Act (Chapter 440 of the Laws of Malta) as:

"…any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data is also defined in the same Act as meaning:

"…personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life"

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Office of the Data Protection Commissioner
Airways House
Second Floor
High Street
Sliema SLM 1549
Malta
T +356 2328 7100
F +356 23287198
idpc.info@gov.mt
www.dataprotection.gov.mt

The Information and Data Protection Commissioner ("**Commissioner**") has the function (among others) of generally ensuring the correct processing of personal data in order to protect individuals from violations of their privacy.

REGISTRATION

Controllers of data (defined in the Act as persons who alone or jointly with others determine the purposes and means of the processing of personal data), unless exempted by the Commissioner in the circumstances mentioned in the Act or in the circumstances mentioned in Subsidiary Legislation 440.02, must generally notify the Commissioner before carrying out wholly or partially automated processing operations or a set of such operations which are intended to serve either a single or several related purposes. The Commissioner maintains a Register of processing operations which have been notified to him.

The Register must contain the following information:

- the name and address of the data controller and of any other person authorised by him in that respect, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed; and
- proposed transfers of data to third countries.

DATA PROTECTION OFFICERS

Under Maltese law there is no obligation to appoint data protection officers. However, the Act states that the controller of personal data shall notify the Commissioner on the appointment or removal of a personal data representative (if any). The personal data representative has the function (among others) of independently ensuring that the controller processes personal data in a lawful and correct manner and in accordance with good practice and in the event of the personal data representative identifying any inadequacies, he shall bring these to the attention of the controller.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

Personal data may be processed (which includes also the collection of data) only if:

- the data subject has unambiguously given his consent;
- processing is necessary for the performance of a contract to which the data subject is a party to or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed; or
- processing is necessary for a purpose that concerns a legitimate interest of the controller, or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

If the data subject gives notice to the controller of his opposition, personal data cannot be processed for the purposes of direct marketing.

As a general rule, sensitive personal data cannot be processed except in the cases mentioned in the Act (e.g. where the data subject has given his explicit consent to processing or has made the data public).

The data subject has a right to be provided, by the controller or any person authorised by him, with information such as the identity and habitual residence, or principal place of business, of the controller and of any other person authorised by him in that respect; the purpose of the processing; and any further information relating to matters such as the recipients of the data, whether the reply to any questions made to the data subject is obligatory or voluntary and the existence of the right to access, rectify and erase the data concerning him. The controller must guarantee fair processing in respect of the data subject.

TRANSFER

The controller must notify the Commissioner of any proposed transfers of data to third countries, since such transfers also constitute 'processing' under Maltese law. 'Third countries' only include countries which are not Member States of the European Union. The transfer may only take place if the third country to which the data is to be transferred ensures an adequate level of protection. Whether the country ensures such a level of protection shall be decided by the Commissioner.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

A transfer of data to a third country that does not ensure an adequate level of protection may still be effected by the controller but only if the data subject gives his unambiguous consent to the proposed transfer or if the transfer:

- is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's request;
- is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;
- is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims;
- is necessary in order to protect the vital interests of the data subject; or
- is made from a register that according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided that the conditions laid down in law for consultation are fulfilled in the particular case.

In these cases the Commissioner's approval is not required but the transfer must still be notified.

The Commissioner has the power to authorise such a transfer of personal data to a third country that does not ensure an adequate level of protection provided however that the controller provides adequate safeguards, such as by contractual provisions, with respect to the protection of privacy and fundamental human rights.

The Minister responsible for freedom of information and data protection may also designate by Order, in order to implement any international convention to which Malta is party or any other international obligation of Malta, that the transfer of personal data to any country listed in the Order shall not be restricted on grounds of protection of privacy.

Apart from notification to the Commissioner, no other restrictions or formalities apply in relation to transfer of personal data to:

- Member States of the European Union;
- Member States of the EEA;
- Third countries which are recognised by the EU Commission to have an adequate level of protection; or
- Organisations complying with the US Safe Harbor privacy principles.

SECURITY

Data controllers must implement the appropriate technical and organisational measures to protect personal data which is processed against accidental destruction or loss or unlawful forms of processing. An adequate level of security must be provided which gives regard to:

- the technical possibilities available;
- cost of implementing the security measures;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- special risks that exist in the processing of personal data; and
- sensitivity of the personal data being processed.

If a processor is engaged by the controller, the controller must ensure that the processor can implement the necessary security measures and that the processor actually takes such measures.

BREACH NOTIFICATION

Legal Notice 239 of 2011, which will soon come into force, will amend Subsidiary Legislation 440.01, Processing of Personal Data (Electronic Communications Sector) Regulations, making new provisions for breach notifications.

The Regulations will provide (after the amendments have been brought into force) that, in the case of a personal data breach, the provider of publicly available electronic communications service must notify the breach to the Commission without delay. "Personal data breach" will be defined in the Regulations as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service*".

If the breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider must also notify the subscriber or individual of the breach without delay. However, notification to the subscriber or individual concerned shall not be required on the condition that the provider demonstrates to the satisfaction of the Commissioner that he has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the security breach. Such technological protection measures should render the data unintelligible to any person who is not authorised to access it.

If the provider has not already notified the subscriber or individual of the personal data breach, the Commission may require the provider to do so after considering the likely adverse effects of the breach.

The notification to the subscriber or individual must at least include the nature of the breach and the contact points where more information can be obtained. The notification must also recommend measures to mitigate the possible adverse effects of the breach.

The notification to the Commission shall also include the consequences of and the measures proposed or taken by the provider to address the breach.

The Regulations will also provide that the Commissioner is to encourage the drawing up of guidelines and where necessary issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format which such notification is to take and the manner in which the notification is to be made.

Service providers are to maintain an inventory of personal data breaches consisting of the facts surrounding the breach, its effects and the remedial action taken which must be sufficient so as to enable the Commissioner to verify compliance with the provisions of the Regulations.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

The Act states that any person who does not comply with any lawful request relevant to an investigation by the Commissioner shall be guilty of an offence under the Act.

In the exercise of his functions under the Act, the Commissioner has the same powers to enter and search any premises as are vested in the executive police by any law as may be in force from time to time.

If the Data Protection Commissioner concludes that personal data is processed or may be processed in an unlawful manner, the Commissioner shall order rectification, and if rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data to continue processing the personal data in any manner other than to store that data.

If the controller does not implement security measures in terms of the Act, the Data Protection Commissioner may impose an administrative fine.

Where the Data Protection Commissioner decides that personal data has been unlawfully processed, the said Commissioner shall by notice order the controller of personal data to erase the personal data. If the controller of personal data feels aggrieved by the decision of the Commissioner, he may, by application, request the Court of Appeal of Malta to revoke the order of the Commissioner.

The data subject may, by sworn application filed in the court, exercise an action for damages against the controller who processes data in contravention of the Act or regulations made there under.

In addition, any person who provides untrue information to data subjects as is prescribed by the Act, or in the notification to the Commissioner; or processes personal data in contravention of the provisions of the Act; or transfers personal data to a third country in contravention of the Act; or omits to give notification under the provisions of the Act or any regulation issued there under, shall be guilty of an offence and shall on conviction be liable to a fine (multa) not exceeding EUR 23,293.73 or to imprisonment for six months or to both.

Any person aggrieved by a decision of the Commissioner shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within thirty days from the notification to him of the said decision.

Any party to an appeal to the said Tribunal who feels aggrieved by a decision of the Tribunal, or the Commissioner if he feels aggrieved with any such decision, may on a question of law appeal to the Court of Appeal of Malta within thirty days from the date on which that decision has been notified.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

The Act applies also to most electronic marketing activities since in the course of such activities, it is likely that 'personal data' as defined above (including e-mails) will be 'processed' as understood by the Act. In relation to direct marketing (even electronic), consent may be revoked at will by the data subject(s). The Controller is legally bound to inform the data subject that he/she may oppose such processing at no cost.

Apart from the Act, the 'Processing of Personal Data (Electronic Communications Sector) Regulations 2003' (Legal Notice 16 of 2003 as amended) (the 'Electronic Communications Regulations') address a number of activities relating specifically to electronic marketing.

In the case of subscriber directories, the producer of such directories shall ensure (without charge to the subscriber) that before any personal data relating to the subscriber (who must be natural persons) is inserted in the directory, the subscriber is informed about the purposes of such a directory of subscribers and its intended uses (including information regarding search functions embedded in the electronic version of the directories). No personal data shall be included without the consent of the subscriber. In furnishing his consent the subscriber shall determine which data is to be included in the directory and he is free to change, alter or withdraw such data at a later date. The personal data which shall be used in the directory must be limited to what is necessary to identify that subscriber and the number allocated to him, unless the subscriber has given his additional consent authorising the inclusion of additional personal data.

The Electronic Communications Regulations also deal with the issue of unsolicited communications. A person is prohibited from using any publicly available electronic communications service to engage in unsolicited communications for the purpose of direct marketing by means of:

- an automatic calling machine
- a facsimile machine, or
- electronic mail, to a subscriber, irrespective of whether such subscriber is a natural person or a legal person, unless the subscriber has given his prior explicit consent in writing to the receipt of such a communication.

By way of exception to the above, where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the Act that same person may use such details for direct marketing of its own similar products or services. However, the customers must be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

In all cases the practice of sending electronic mail for the purposes of direct marketing, disguising or concealing the identity of the sender or without providing a valid address allowing the recipient to send a request requesting that such communication cease, is strictly prohibited.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookie Compliance – Legal Notice 239 of 2011 entitled 'Processing of Personal Data (Electronic Communications Sector)(Amendment) Regulations 2011 is yet to enter into force. Once brought into force, this Legal Notice would amend present regulations thereby implementing into Maltese Law the amendments under Article 2(5) of Directive 2009/136/EC. These regulations shall enter into force on such date as the Minister responsible for data protection shall determine by notice in the Malta Government Gazette. We have no indication of when such date may be although we expect that this will occur in the not-so-distant future.

Traffic Data – In terms of the Electronic Communications Regulations', traffic data relating to subscribers and users processed by an undertaking which provides publicly available electronic communications services or which provides a public communications network, shall be erased or made anonymous when it is no longer required for the purpose of transmitting a communication.

Traffic data required for the purposes of subscriber billing or interconnection payments may be retained provided however that the retaining of such data shall only be permissible up to the period during which the bill may be lawfully challenged or payment pursued.

Furthermore, traffic data may be processed where the aim is to market or publicise the provision of a value-added service, however, the processing of such data shall only be permissible to the extent and for the duration necessary to render such services.

Processing of traffic data is also permissible by an undertaking providing publicly available electronic communication for the following purposes:

- managing billing or traffic management;
- customer enquiries;
- fraud detection; or
- rendering of value-added services.

Location Data – where location data (other than traffic data) relating to users of subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision a value-added service.

Prior to obtaining the user or subscriber's consent, the undertaking providing the service shall inform them of the following:

- the type of location data which shall be processed;
- the purpose and duration of processing; and
- whether the processed data shall be transmitted to a third party for the purpose of providing the value-added service

A user and/or subscriber may withdraw their consent for the processing of such location data (other than traffic data) at any time.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

34. MAURITIUS

CONTRIBUTION DETAILS

Conyers Dill & Pearman (Mauritius) Limited
Level 3, Tower I
Nexteracom Towers
Cybercity, Ebene
Mauritius

Ashvan Luckraz
ashvan.luckraz@conyersdill.com

Stephen Scali
stephen.scali@conyersdill.com

LAW

Data Protection Act 2004 (the "**MU DPA**") was enacted for the protection of the privacy rights of individuals in response to the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals. The MU DPA came into operation in February 2009. Data Protection Regulations were issued in 2009 by the Data Protection Office. It also is responsible for ensuring compliance with the Data Protection Act and bringing enforcement actions.

DEFINITION OF PERSONAL DATA

"Personal data" means –

(a) data which relate to an individual who can be identified from those data; or

(b) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion.

DEFINITION OF SENSITIVE PERSONAL DATA

"Sensitive personal data" means personal information concerning a data subject that include information as to:

- the racial or ethnic origin;
- political opinion or adherence;
- religious belief or other belief of a similar nature;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- membership to a trade union;
- physical or mental health;
- sexual preferences or practices;
- the commission or alleged commission of an offence; or
- any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Office
4th Floor
Authority
Emmanuel Anquetil Building
Corner Sir Virgil Naz & Sir William Newton Streets
Port Louis
Republic of Mauritius
T 230 201 3604
F 230 201 3976

REGISTRATION

Every data controller (and, in principle every data processor) must:

- apply for registration in writing to the Commissioner; and
- together with the application, provide the particulars specified, in the case of a data controller, in section 35 of the MU DPA and, in the case of a data processor, in section 35A of the MU DPA.

Subject to Part VII of the MU DPA (which sets out sections of the MU DPA to which data controllers are exempt from), the MU DPA shall apply to a data controller

- who is established in Mauritius and processes data in the context of that establishment; and
- who is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purpose of transit through Mauritius.

A data controller, who is not established in Mauritius, shall nominate for the purposes of this Act, a representative established in Mauritius.

A Controller will be treated as being established in Mauritius if:

- they are ordinarily resident in Mauritius; or
- they carry out data processing activities through an office, branch or agency in Mauritius.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

An application for registration as a data controller must contain: (i) a description of the personal data being, or to be, processed by or on behalf of the data controller; (ii) the category of data subjects to which the personal data relates; (iii) specify whether or not he holds or is likely to hold sensitive personal data; (iv) a description of the purpose for which the personal data is being or is to be processed; and (v) a description of the recipient(s) to whom the data controller intends, or may wish, to disclose the personal data.

The MU DPA also requires that data processors be registered with the Data Protection Office. However, the relevant regulations setting out the procedure to be followed for such registration have not been issued. Thus, for the time being, in practice, data processors do not need to be registered for the time being.

Where any data controller or data processor intends to keep or process personal data or sensitive personal data for two or more purposes, it must apply a separate registration form for each purpose.

The Commissioner shall grant an application for registration, unless he reasonably believes that:

- the particulars proposed for inclusion in an entry in the register are insufficient or any other information required by the Commissioner either has not been furnished, or is insufficient;
- appropriate safeguards for the protection of the privacy of the data subjects concerned are not being, or will not continue to be, provided by the data controller; or
- the person applying for registration is not a fit and proper person.

DATA PROTECTION OFFICERS

There is no formal requirement for organisations to appoint a data protection officer in Mauritius.

However, in practice, for the purposes of registration of a data controller with the data protection office, a compliance person will need to be designated for every organisation.

COLLECTION AND PROCESSING

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

- the data subject consents;
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party;
- processing of data is required for the performance of a contract to which the data subject is a party; or in order to take steps required by the data subject prior to entering into a contract;
- the processing protects the data subject's vital interests;
- the processing is required for compliance with any legal obligation to which the data controller is subject;
- processing is needed for the administration of justice; or
- processing is needed in the public interest.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The conditions for processing of sensitive personal data include most of the above conditions, but contain an additional list of more stringent conditions that must also be satisfied, such as compliance with a legal obligation to which the data controller is subject; processing that does not involve the disclosure of the personal data to a third party unless the consent of the data subject has been obtained; or where the processing is required by law.

Whichever of the above conditions is relied upon, the data controller must provide the data subject with "fair processing information" notice. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair and lawful.

TRANSFER

Personal data must not be transferred to a third country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data. Adequacy of the level of protection of a country is assessed by considering all the circumstances surrounding the transfer, in particular the nature of the data, purpose and duration of the proposed processing, country of origin and country of final destination, rules of law, both general and sectorial in force in the country in question and any relevant codes of conduct or other rules and security measures which are complied with in that country.

However, personal data transfers to third countries are permissible if:

- the data subject consents;
- the transfer is necessary;
  - for the performance of or for entering into a contract between the data subject and the data controller;
  - for the conclusion of or performance of a contract between the data controller and a third party if the contract serves the data subject's interests; or
  - in the public interest, to safeguard public security or national security.
- the transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.

In all cases, a data controller cannot transfer personal data to another country, except with the written authorisation of the Commissioner.

SECURITY

Data controllers must take appropriate security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of personal data. The measures must ensure a level of security appropriate to the nature of the personal data and the harm which might result from the unauthorised access to, alteration of, disclosure of, destruction of the data and its accidental loss.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Where a data controller is using the services of a data processor, he must choose a data processor providing sufficient guarantees regarding security and organisational measures.

In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a data controller must have regard to (a) the state of technological development available; (b) the cost of implementing any of the security measures; (c) the special risks that exist in the processing of the data; and (d) the nature of the data being processed.

BREACH NOTIFICATION

The MU DPA provides for an option to make a complaint to the Commissioner in cases of actual or potential contraventions of the MU DPA or of its regulations. However, there is no mandatory requirement in the MU DPA to report data security breaches or losses to the Data Protection Office or to data subjects.

The guidelines issued by the Data Protection Office however provide that if a privacy breach creates a risk of harm to the individual, those affected should be notified so as to mitigate the damage caused or likely to be caused by such harm.

ENFORCEMENT

The Commissioner is responsible for the enforcement of the MU DPA.

In cases where the Commissioner is of opinion that a data controller or a data processor has contravened, is contravening or is about to contravene the MU DPA, the Commissioner may serve an enforcement notice on the data controller or the data processor requiring him to take such steps within such time as may be specified in the notice.

The Commissioner can apply to a Judge in Chambers for an order for the expeditious preservation of data ("**preservation order**") where he has reasonable grounds to believe that such data is vulnerable to loss or modification.

The Commissioner can also carry out prior security checks in relation to processing of data, and periodic audits of the systems of data controllers to ensure compliance with data protection principles specified under the First Schedule of the MU DPA. It must be noted that on completion of an investigation under the MU DPA, the Commissioner must, where the investigation reveals that an offense has been committed under the MU DPA or the Regulations, refer the matter to the Police.

A data controller who knowingly supplies false information in relation to particulars furnished (further to his registration with the Data Protection Office) commits an offence and will, on conviction, be liable to a fine not exceeding Rs. 100,000 and to imprisonment for a term of up to 2 years.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

If a data controller or data processor does not comply with an enforcement notice (as provided for under the MU DPA) he may be liable for a fine of up to Rs. 50,000 and to imprisonment for a term of up to 2 years.

The MU DPA provides that any person who contravenes the MU DPA commits an offence. Where no specific penalty (e.g. in cases of unlawful disclosure of data) is provided for an offense, the person will on conviction, be liable for a fine of up to Rs. 200,000 and to imprisonment for a term of up to 5 years.

In addition to any penalty, the Court may (a) order the forfeiture of any equipment or any article used or connected in any way with the commission an offense; (b) order or prohibit any act to stop a continuing contravention.

ELECTRONIC MARKETING

The MU DPA will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be "personal data" for the purposes of the MU DPA). The MU DPA does not prohibit the use of personal data for the purposes of electronic marketing, but provides individuals with the right to prevent the processing of their personal data (e.g. a right to "opt out") for use of their personal data for direct marketing purposes.

A person may, at any time, by notice in writing, ask a data controller to cease, or not to begin, the processing of personal data for the purposes of direct marketing. Where the data controller receives such a request, it must, as soon as reasonably practicable and in any event not more than 28 days after the request has been received:

- erase the data at locations where the personal data are kept only for purposes of direct marketing; and
- where the data are kept for direct marketing and another purpose, stop processing the data for direct marketing.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Mauritius law does not contain special provisions relating to online privacy.

Whilst Mauritius law does not contain special provisions relating to online privacy, please find set out below guidelines that have been issued by the Commissioner in relation thereto.

Part IV of the MU DPA sets out the obligations to collect personal data in a responsible way by imposing through section 22, the duty to inform the user/s of the identity of the data controller, the purposes for which the data are being collected, the intended recipients or beneficiaries of the data, whether the express consent of the user/s is/are required for the collection and the right of the user/s to access the data, amongst others. Section 27 further provides for the duty of the data controller to cater for appropriate security and organisational measures in order to protect the processing or collection of the data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Pursuant to the general obligations provided under the MU DPA, the user should be informed when a cookie is intended to be received, stored or sent by the internet software. The message should specify, in clear terms, which personal information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie.

On establishing a connection with a web server (sending a request or receiving a web page), the user must be informed which information is intended to be transferred and for what purposes. Hyperlinks are also sent by a website to a user, and the user's browser should be able to reveal them all to the user.

The MU DPA is also applicable when behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles which, in most cases, are personal data.

Ad network providers should create prior opt-in mechanisms. Mechanisms to deliver informed, valid consent should require an affirmative action by the data subject indicating his/her willingness to receive cookies and the subsequent monitoring of his/her surfing behaviour for the purposes of sending him/her tailored advertising.

A user's acceptance to receive a cookie could also entail his/her acceptance for the subsequent readings of the cookie, and hence for the monitoring of his/ her internet browsing. It would not be necessary to request consent for each reading of the cookie.

However, to ensure that data subjects remain aware of the monitoring over time, ad network providers should:

- limit in time the scope of the express consent;
- offer the possibility to easily revoke their consent to being monitored for the purposes of serving behavioural advertising; and
- create a symbol or other tools which should be visible in all the web sites where the monitoring takes place (the website partners of the ad network provider). This symbol would not only remind individuals of the monitoring but also help them to control whether they want to continue being monitored or wish to revoke their consent.

Network providers should ensure compliance with the purpose limitation principle and security obligations. Ad network providers should implement retention policies which ensure that information collected each time that a cookie is read is automatically deleted after a justified period of time necessary for the purposes of the processing.

Ad network providers are bound by the obligations of data controllers insofar as they place cookies and/or retrieve information from cookies already stored in the data subjects' terminal equipment and determine the purposes and the essential means of the processing of data. Ad network providers have complete control over the purposes and means of the processing.

Publishers will be joint controllers if they collect and transmit personal data regarding their visitors such as name, address, age, location, etc to the ad network provider. To the extent that publishers act as data controllers or processors, they are bound by the obligations arising under the MU DPA regarding the part of the data processing under their control.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Social Networking Site ("**SNS**") providers and third party application providers are typically data controllers with corresponding responsibilities towards users. Section 54 of the MU DPA on 'Domestic purposes" will apply to SNS such that personal data processed by an individual for his personal, family or household affairs or for recreational purposes would be exempt from certain provisions of the Act. The dissemination and use of information available on SNS for other secondary, unintended purposes is of key concern to the Data Protection Office. Robust security and privacy-friendly default settings are advocated throughout the guide as the ideal starting point with regard to all services on offer.

The express consent of the user must be sought for all use/s of his/her data including profile enrichment exercises. Opt-outs facilities must be provided by search engines and requests from users to update/refresh caches must be complied with.

Search engines may only process personal data for lawful and necessary purposes and the amount of data has to be relevant and not excessive in respect to the various purposes to be achieved.

Search engine providers must delete or anonymise personal data in an irreversible manner once they are no longer necessary for the purpose for which they were collected.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

35. MEXICO (UNITED MEXICAN STATES)

CONTRIBUTION DETAILS

Carlos Valencia
Partner
T +52 55.5002.8101
carlos.valencia@dlapiper.com

LAW AND REGULATIONS

The Federal Law on Protection of Personal Data held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de Particulares*) (the "**Law**") was enacted and entered into force on 6 July 2010.

The Executive Branch issued (i) the Regulations to the Law (*Reglamento de la Ley Federal de Protección de Datos en Posesión de Particulares*) on 21 December 2011 (the "**Regulations**"), which entered into force on December 22, 2011, (ii) the Privacy Notice Guidelines on January 17, 2013 (the "**Guidelines**") which will enter into force on 18 April 2013, and (iii) the Parameters for Mandatory Self-Regulation on 17 January 2013 (the "**Parameters**") which entered into force on 18 January 2013. References to the Law throughout this document include the Regulations, the Guidelines and the Parameters.

The Law applies to personal data and sensitive personal data (see definitions below): (i) processed in a facility of the data controller located in Mexican territory; (ii) processed in any facility regardless of its location if the processing is performed on behalf of a Mexican data controller; (iii) where the Law and the Regulations are applicable as a consequence of Mexico's adherence to an international convention (even where the data user is not located in Mexico); or (iv) where the data controller is not located in Mexican territory but uses means located in Mexico to process personal data located abroad. However, when personal data is only in transit through, and is not processed in, Mexico, the Law does not apply.

The Law is limited in its application to the private sector, and does not apply to the government.

DEFINITION OF PERSONAL DATA

"*Personal Data*" means any information concerning an identified or identifiable individual. Unless otherwise noted in this document, personal data includes sensitive personal data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

"*Sensitive Personal Data*" means personal data touching on the most intimate areas of the data subject's life, or data the misuse of which may lead to discrimination or serious risk to the data subject. Specifically, the definition includes data which may reveal items such as racial or ethnic origin, present or future health status, genetic information, religious, philosophical or moral beliefs, union affiliation, political views, and sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

The Federal Institute for Access of Information and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos (IFAI)*) ("**IFAI**") and the Ministry of Economy (*Secretaría de Economía*).

REGISTRATION

Not required.

DATA PROTECTION OFFICERS

All data controllers are required by Law to designate a personal data officer or department (jointly hereinafter referred to as the "Data Protection Officer") to handle requests from any data subjects (called "Data Owners") exercising their rights under the Law. Data Protection Officers are also required to promote the protection of Personal Data within their organizations.

Data controllers located outside Mexico who process personal data of Mexican data subjects abroad must appoint a representative or set up a sufficient alternative mechanism to comply with all aspects of the Law (e.g. comply with "ARCO" rights discussed below).

COLLECTION AND PROCESSING

The term "processing" is broadly defined to include the procurement, use, access, management, transfer, disposal, disclosure or storage of personal data of an identified or identifiable individual by any means

Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data, – i.e. reliance on the assumption that the personal data provided by the data subject will be treated as agreed upon by the parties (in the privacy notice or otherwise) and in compliance with the Law.

To process personal data, data controllers must provide a privacy notice (*Aviso de Privacidad*) (the "**Privacy Notice**"), which must be made available to a data subject prior to the collection and processing of his or her personal data. The Privacy Notice may be provided to data subjects in printed, digital, visual or audio formats, or any other technology.

The Privacy Notice must contain: (i) the identity and domicile of the data controller collecting the data; (ii) the purposes of the data processing; (iii) the options and means offered by the data controller to data subjects to limit the use or disclosure of data; (iv) the means for

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

exercising rights of access, correction, cancellation or objection in accordance with the provisions of the Law; (v) where appropriate, the types of data transfers to be made; and (vi) the procedure and means by which the data controller will notify the data subjects of changes to the Privacy Notice. For transfers, the Privacy Notice must contain the name of the transferee or the person to whom the information is transferred.

The Guidelines consider three forms of privacy notice: comprehensive, simplified and short-form, depending on whether the data is personally obtained from the data subject, the data is obtained directly or indirectly from the data subject or the space to obtain data is minimal or limited (where the space allotted for the gathering of personal data or the Privacy Notice is also minimal or limited), respectively. Each of these forms must meet specific disclosure requirements. The Privacy Notice must be drafted in simple, clear and comprehensible terms, contain all necessary information specified above, and be available in Spanish. The Privacy Notice must be made available to the data subject prior to the collection of the data, at first contact if obtained indirectly or prior to their use when obtained indirectly and no contact is required with the data subject. There are some exceptions to the requirement to provide a subsequent Privacy Notice, such as when the data will be used for scientific, statistical or historical purposes. The data controller has the burden of proof to show that the Privacy Notice was provided.

Personal data must be collected and processed in a lawful manner, in accordance with the provisions of the Law and Regulations, and may not be obtained through deceptive means.

Consent is required for all processing of personal data, except as otherwise provided by the Law. Implicit consent (notice and opt out) applies to the processing of personal data. Express consent (notice and opt in) applies to the processing of financial or asset data and Sensitive personal data, unless an exception applies. With respect to personal data, consent may be communicated verbally, in writing, by electronic or optical means, via any other technology, or by any other unmistakable indications. However, a Data Controller must obtain express written consent from the data subject for any processing of Sensitive Personal Data; written consent may be obtained through the data subject's written signature, electronic signature, or any other authentication mechanism set up for such purpose.

Further, databases containing sensitive personal data may not be created unless justified by legitimate, concrete and consistent purposes, in furtherance of the explicit objectives or activities pursued by the data controller.

Exceptions to the consent requirement for processing of personal data, including sensitive personal data, apply where: (i) exempted by other legislation; (ii) the data is contained in publicly available sources; (iii) the identity of the data subject has been disassociated from the data; (iv) processing is for the purpose of discharging obligations under a pre-existing relationship between the data subject and the data controller; (v) there is an emergency situation that could potentially harm an individual with regard to his person or property; (vi) processing is essential for medical attention, prevention, diagnosis, health care delivery, medical treatment or health services management, where the data subject is unable to give consent in the manner established by the General Health Law (*Ley General de Salud*) and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

other applicable laws, and said processing is carried out by a person subject to a duty of professional secrecy or an equivalent obligation; or (vii) pursuant to resolution issued by a competent authority.

Processing of personal data must be limited to the fulfilment of the specific purposes set out in the Privacy Notice. If the personal data is used for a purpose not identified in the Privacy Notice, consent of the data subject is required anew.

Databases containing sensitive personal Data may be created only: (i) where necessary to comply with a legal requirement; (ii) where justified for purposes of national security, public order, public health, or for the protection of third party rights; or (iii) when the data controller is compelled to create it for a legitimate and specific purposes.

The data controller must ensure that Personal Data contained in databases are relevant, correct and up to date for the purposes for which they has been collected. When the personal data are no longer necessary for the fulfilment of the objectives set forth in the Privacy Notice and applicable laws, they must be eliminated.

The Data Controller must also, among other things, implement privacy policies and mandatory privacy programs, set up supervisory systems, update and inform its personnel about matters regarding protection of Personal Data, and set up procedures to receive and process complaints and resolve questions from data subjects.

TRANSFER

The data controller may freely transfer personal data to domestic or foreign third parties, if the Privacy Notice so provides and the data subject has not opted out. Details regarding the transfers (recipient of the personal data, purposes of the transfer, etc.) of personal data must be provided under the Privacy Notice.

Any third party receiving personal data assumes the same obligations as the data controller that transferred the personal data. Except for disclosures to data processors, personal data may only be transferred for the purposes authorised by the data subject's consent to the Privacy Notice, which must be opt out or opt in depending on whether the information is personal data or sensitive personal data, respectively.

Domestic or international transfers of personal data may be carried out without the consent of the data subject where: (i) the transfer is pursuant to a law or treaty to which Mexico is party; (ii) the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; (iii) the transfer is made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies; (iv) the transfer is necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject; (v) where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; (vi) where the transfer is necessary for the recognition, exercise or defence of a right in a judicial proceeding; and (vii) where the transfer is necessary to maintain or comply with an obligation binding on the data controller and the data subject.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The Regulations distinguish between domestic and international transfers of personal data. For international transfers of personal data, the third party receiving the personal data must enter into an agreement or other instrument with the data controller to ensure the lawful processing of the personal data in compliance with the Law. The transfer of personal data between or among related corporate entities is allowed for specific purposes as long as those purposes are mentioned and disclosed to the data subject in the Privacy Notice. If the personal data is intended to be used for purposes other than those indicated in the Privacy Notice, then express consent must be obtained from the data subject anew.

SECURITY

All responsible 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 unauthorised use, access or processing. Data processors may not adopt security measures with respect to personal data that they process on behalf of a data controller that are inferior to those which the processor has in place to manage its own information. The sufficiency of the security measures will be assessed in relation to the risk involved, potential consequences for data subjects, sensitivity of the data, and technological developments. The Regulations set out criteria that must be considered by the data controller in determining the appropriate security measures and actions to protect the Personal data, and require data controllers to periodically review and update their security measures. The IFAI may also issue non-binding recommendations to data controllers for securing personal data when the data controller's security measures are insufficient or may put the personal data in risk.

Data controllers or third parties involved in any stage of personal data processing must maintain the confidentiality of the data, and this obligation continues even after the end of any relationship with the data subject or with the data controller.

Any third party who is in charge of securing personal data on behalf of the data controller ("**Third Party**") is subject to the same obligations as the data controller to protect the data. The Third Party shall; (i) process the personal data only in accordance with the instructions of and purposes indicated the data controller; (ii) set up security measures to protect the personal data; (iii) keep the personal data confidential; (iv) eliminate the personal data once the legal relationship between the data controller and the third party is terminated; and (v) refrain from transferring personal data, except where (a) the data controller instructs it to do so; (b) the transfer is made to a subcontractor; or (c) the personal data is requested by an authority.

BREACH NOTIFICATION

Security breaches occurring at any stage of processing that materially affect property or Sensitive personal data must be promptly reported by the data controller to the data subject, so that the data subject can take appropriate action to defend his or her rights.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The Regulations provide that breach notification must include at least the following information; (i) a description of the issue; (ii) the personal data that was exposed to the security breach, (iii) recommended actions to the data subject on how to protect his/her own interests and to secure the personal data; (iv) the corrective actions that the data controller will take immediately, and (v) the process pursuant to which the data subject may obtain additional information regarding the data breach, and any information mentioned in the notice to protect his/her interests, the actions to be taken by the data controller to mitigate any harm or damage and the recommendations of the data controller to the data subject on how to mitigate the effect of the breach.

ENFORCEMENT

The provisions of the Law are mandatory, and apply to data controllers and any other person processing personal data. the ifai may act *ex-officio* or in response to complaints regarding violations of the law. if any breach of the law or the regulations is alleged, the IFAI may perform on site inspections at the data controller's facilities to verify compliance with the Law. Inspections may last up to 180 days.

Data subjects can enforce their access, correction, cancellation and objection rights ("**ARCO Rights**") via the IFAI and ultimately the court system.

Violations of the Law may result in either monetary penalties or imprisonment.

- The IFAI may impose monetary fines from 100 to 320,000 times the Mexico City minimum wage (approximately US$480 to US$1,534,275, based upon an exchange rate of MxP$13 per US$1). With regard to violations committed concerning the processing of sensitive personal data, sanctions may be increased up to double these amounts.
- Three months to three years imprisonment may be imposed on any person authorised to process personal data who, for profit, causes a security breach affecting the databases under its custody. Penalties are doubled for sensitive personal data.
- Six months to five years imprisonment may be imposed on any person who, with the aim of obtaining unlawful profit, processes personal data deceitfully, taking advantage of an error of the data subject or a person authorised to transmit such data. Penalties are doubled for sensitive personal data.

Data controllers may adopt self regulation mechanisms, such as codes, policies, rules and, standards, or become part of incorporated or unincorporated self-regulatory bodies to support their compliance with the provisions of the Law; these self-regulation standards become binding on Data Controllers and provide *prima facie* evidence that the Data Controller is in compliance with the Law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The implementation of the self-regulation mechanisms is regulated at length by the Parameters. The Parameters intend to foster compliance by data controllers with the Regulations, and incentivize the data controllers to apply for certification by the IFAI or other certifying organisms. The Parameters set forth the components that, at a minimum, must be addressed in any self-regulatory mechanism, including, scope, duration, internal updating mechanisms, ARCO rights enforcement, alternate dispute resolution, and form agreements. The Parameters also address the certification system.

ELECTRONIC MARKETING

Email marketing constitutes the processing of persona data and is subject to the Privacy Notice and opt-out consent requirements of the Law.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The Guidelines which address the use of cookies, web-beacons and other analogous technologies, require that when a data controller uses online tracking mechanisms that permit the automatic collection of personal data, the Privacy Notice must include; a prominent warning to the data subject of the use of such technologies; the fact that personal data is being gathered; and the option to disable such means (unless they are necessary for technical reasons). The notice must also specify the type of personal data being gathered and the purpose.

However, an IP address alone is not likely to rise to the level of personal data under the Law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

36. MONACO

CONTRIBUTION DETAILS

Gordon S. Blair Law Offices
www.gordonblair.com

Geneviève Pace
Principal
genevieve.pace@gordonblair.com
T +377 93 25 00 52

LAW

Data protection in Monaco is regulated by Data Protection Law n° 1.165 of 23 December 1993, modified by Law n° 1.353 of 4 December 2008 ("**DPL**").

Furthermore, the Principally of Monaco is part of the Council of Europe and entered into Convention n° 108 of the European Council.

The Principality of Monaco is not part of the EU and as a consequence did not transpose Data Protection Directive 95/46/EC.

DEFINITION OF PERSONAL DATA

Personal data is defined under the Data Protection Law as: "*data enabling identification of a determined or indeterminable person. Any individual who can be identified, directly or indirectly, notably by reference to an identification number or to one or more factors specific to his physical, psychological, psychical, economical, cultural, or social identity is deemed to be identifiable*".

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data is not expressly defined under the DPL but it is deemed to be: "*Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health/genetic data, sex life, data concerning morals or social matters*".

NATIONAL DATA PROTECTION AUTHORITY

The Monegasque regulator is the Commission for Control of Personal Data ("**Commission de Contrôle des Informations Nominatives**" or "**CCIN**").

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

Data controllers who process personal data must inform/notify/request approval from the CCIN so that their processing of personal data may be registered. Any changes to the processing of personal data will require the registration to be amended.

The notification should include the following information:

- what data is being collected;
- why the data will be processed;
- the categories of data subject; and
- whether the data will be transferred either within or outside the Monaco.

DATA PROTECTION OFFICERS

There is no requirement in Monaco for organisations to appoint a data protection officer.

However, appointing a data protection officer is well perceived by the CCIN as evidence of the company's actions to ensure compliance with the data protection legislation; however, in practice, companies in Monaco do not appoint data protection officer in generals.

COLLECTION AND PROCESSING

Data processing must be justified by:

- data subject's consent;
- a legal duty imposed to the data controller;
- a public purpose;
- completion of a contract entered into between the data controller and the data subject; or
- data controller's legitimate interest subject not to fail to respect data subject's fundamental rights and liberties.

Where sensitive personal data is processed, one of the above conditions must be met plus one from an additional list of more stringent conditions.

The data controller must also provide the data subject with "fair processing information". This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

As the Principality of Monaco is not part of the EU, the DPL does not distinguish between EEA jurisdictions and non EEA jurisdictions.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

However, the DPL provides that the transfer of data is authorised for cross border access, storage and processing of data only to a country with equivalent protection and reciprocity.

The CCIN has established a list of the countries deemed to have an equivalent protection and reciprocity. States, and parties to Convention of the Council of Europe n° 108 relating to the protection of individuals for personal data automatic processing, are deemed to have the equivalent protection as Monaco.

The declaration to CCIN should indicate whether it is intended for personal data to be transferred cross-border.

The transfer of data to countries that do not provide a sufficient level of protection shall be either:

- accepted by the data subject; or
- necessary for:
  - safety of data subject's life;
  - the protection of public purpose;
  - compliance with obligations relating to the protection of a legal right;
  - public access to information;
  - completion of a contract entered into between the data controller and the data subject;
  - conclusion or completion of a contract entered into or to be entered into between the data controller and a third party in the interest of the data subject; or
- duly authorised by the CCIN under the condition that the data controller and the data recipient provide sufficient guarantees in order to protect fundamental rights and liberties.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data.

BREACH NOTIFICATION

There is no mandatory requirement in the DPL to report breaches or losses to the CCIN or to data subjects.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

The CCIN and Monegasque Courts are responsible for enforcing the DPL. If the CCIN becomes aware that a data controller is in breach of the DPL, he can serve an enforcement notice requiring the data controller to rectify the position. Failure to comply with an enforcement notice is criminal offence and can be punished on conviction of imprisonment of 1 to 6 months or a fine of from Eur 9,000 to Eur 90,000 or both.

ELECTRONIC MARKETING

Prior to implementing any electronic marketing activity the CCIN must be notified, as electronic marketing activities may use personal data. The law does not prohibit the use personal data for the purpose of electronic marketing. However, when implementing electronic marketing activities a company must respect the provisions of article 1, article 10 and article 14 of the DPL

The automated or non-automated processing of personal data must not infringe the fundamental rights and freedoms enshrined in Title III of the Constitution.

Personal data must be:

- collected and processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- accurate and, if necessary, updated; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further processed, is erased or rectified; and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

Processing of personal data must be justified:

- by consent from the data subject(s);
- by compliance with a legal obligation to which the data controller or their representative is subject;
- by it being in the public interest;
- by the performance of a contract or pre-contractual measures with the data subject; or
- by the fulfillment of a legitimate motive on the part of the data controller or their representative or by the recipient, on condition that the interests or fundamental rights and freedoms of the data subject are not infringed.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Persons from whom personal data is collected must be informed:

- of the identity of the data controller and, if applicable, the identity of their representative in Monaco;
- of the purpose of processing;
- of the obligatory or optional nature of replies;
- of the consequences for them of failure to reply;
- of the identity of recipients or categories of recipients;
- of their right to oppose, access and rectify their data; and
- of their right to oppose the use on behalf of a third party, or the disclosure to a third party of their personal data for the purposes of prospection, particularly commercial prospection

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Prior to the use of Traffic Data, Location Data and Cookies the CCIN must be notified. The use of Traffic Data, Location Data and Cookies will have to respect of the provisions of the DPL.

In addition, the data controller or their representative must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss, corruption, unauthorised disclosure or access, in particular where processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Measures implemented must ensure an adequate level of security with regard to the risks posed by processing and by the nature of the data to be protected.

Where the data controller or their representative makes use of the services of one or more service providers, they must ensure that the latter are able to comply with the obligations laid down in the two previous paragraphs.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

37. MOROCCO

CONTRIBUTION DETAILS

Hajji & Associés
28, Bld. Moulay Youssef, Casablanca, 20070, Morocco
T +212 522 48 74 74
F +212 522 48 74 75
http://www.ahlo.ma

Amin Hajji
Partner
a.hajji@ahlo.ma

Myriam Bennani
Partner
m.bennani@ahlo.ma

LAW

Personal data protection is governed in Morocco by the Law n° 09-08 of 18 February 2009 relating to the protection of individuals with respect to the processing of personal data (the "**Law**") and by its implementation Decree n° 2-09-165 of 21 May 2009 ("**Decree**").

DEFINITION OF PERSONAL DATA

Personal data is defined by article 1.1 of the Law as any information of any nature and independently of its format, including the sound and images relating to an identified or identifiable individual, referred to in the Law as a "concerned individual." A person is deemed identifiable when he or she can be identified directly or indirectly, especially by reference to an identification number or one or several specific elements of his or her physical, physiological, genetic, psychical, economic, cultural or social identity.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive data is defined by article 1.3 of the Law as "any information pertaining to a "concerned individual" that reveals racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or that concern sex life or health, including the genetic data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ("**CNDP**") (in English "*National Control Commission for the Protection of Personal Data*")

6 Boulevard Annakhil
immeuble Les Patios
3ème ètage
Hay Riad – Rabat, 10000
Morocco
T +212 537 57 11 24
F +212 537 57 21 41
contact@cndp.ma

REGISTRATION

The processing of personal data requires a prior notification to the CNDP.

The processing of sensitive data or of personal data that includes ID card numbers requires a prior authorization from the CNDP.

The prior notification or authorization application to the CNDP must specify, among other things:

- the purpose(s) of the processing;
- the identity and the address of the data controller (ie the natural or legal person who determines the purpose and the means of the processing of the personal data and either implements such decisions itself or engages a data processor to implement them);
- the possible connections between databases;
- the personal data processed and the categories of persons about whom personal data are processed;
- the time period for which the data will be retained;
- the department or person(s) in charge of implementing the data processing;
- the recipients or categories of recipients of the personal data; and
- the measures taken to ensure the security of the processing. Additional specific security measures are required when processing sensitive data.

DATA PROTECTION OFFICERS

No requirement to appoint a data protection officer.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

Any personal data must be processed consistently with the following general principles;

- all personal data must be processed fairly and lawfully;
- all personal data must be collected for specific, explicit and legitimate purposes and be subsequently processed in accordance with these purposes for which they are collected; and
- all personal data must be accurate, comprehensive and, when necessary, kept up to date.

The processing of personal data shall have received the individual's consent or shall fulfill one of the following conditions;

- processing is required by law;
- the purpose of the processing is to save the individual's life;
- the purpose of the processing is to carry out a public service;
- the processing relates to the performance of a contract to which the concerned individual is a party; or
- the processing relates to achieving a legitimate interest of the data controller, balanced against the interests and fundamental rights and liberties of the concerned individual.

Where sensitive personal data are processed, a different list of specific conditions applies. Indeed, the concerned individual must give his/her express consent for this processing unless the processing meet one of the following conditions;

- the processing is necessary for the exercise of legal or statutory functions of the controller;
- the processing is necessary to protect the vital interests of the concerned individual, and that the concerned individual is in physically or legally incapable to give his/her consent;
- the processing relates to data made public by the concerned individual; or
- the processing regards the recognition, exercise or defense of legal claims and is done exclusively for this purpose.

The person from whom the personal data is collected must receive notice of:

- the identity of the data controller and, if applicable, the data processor;
- the purposes of the data processing; the recipients or categories of recipients of the data; and
- the right to object, for a legitimate reason, to the collection of such data, the right to access the collected data and the right to have the processed data rectified.

TRANSFER

The transfer of a data subject's personal data to another country is allowed if the country provides a sufficient level of protection in relation to an individuals' private life and fundamental rights and liberties. The sufficient nature of the protection is evaluated with regards to national laws and applicable security measures.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Data controllers may transfer personal data out of Morocco to countries that are not deemed to offer adequate protection if the transfer is necessary:

- to safeguarding the individual's life;
- to safeguarding the public interest;
- to comply with obligations relating to the recognition, exercise or defence of a legal right;
- to the consultation of a public register intended to inform the public;
- to the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request; and
- to the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party.

SECURITY

The entity processing the data must take all reasonable precautions with regard to the nature of the data and the risk presented by the processing, in order to preserve the security of the data and, among other things, to prevent third parties' gaining unauthorised access to such data. Where sensitive data are processed, the law sets forth specific security requirements that must be followed.

A data processor may only process personal data based upon the instructions of the data controller. The data processor must provide sufficient guarantees in terms of security and confidentiality. However, the data controller remains liable for the processor's compliance with these obligations.

BREACH NOTIFICATION

The Law does not set out any obligation to notify the CNDP or the concerned individual in the event of a data security breach.

ENFORCEMENT

The CNDP is responsible for enforcing the Law.

Violations of the obligations set forth in the Law are punishable as an administrative and/or criminal offence.

Article 50 to 64 of the Law makes it a violation for any person intentionally to:

- fail to notify or seek CNDP's authorization for data processing;
- provide false information in the notification or in the applications for authorization for the processing of personal data;
- misappropriate or uses personal data in a manner incompatible with the purpose of the collection;
- promote or carry an illegal collection of personal data; or

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- fail to comply with the obligations set forth in the Law or the Decree.

The above offences are punishable by a fine ranging from MAD 10,000 (approx. US$1,200) to MAD 600,000 (approx. US$72,000) and/or imprisonment from three months to four years.

In addition, where the offender is a legal entity, it may be subject to the following penalties:

- partial seizure of its material goods;
- seizure of objects and things whose production, use, carrying, holding or selling is an offense; and
- closure of the entity's premises where the offense was committed.

ELECTRONIC MARKETING

Article 10 of the Law provides that advertising/promotion via any electronic means (eg email, fax, SMS) is forbidden if the recipient has not affirmatively consented to it. However advertising and promotion are allowed when the data were collected directly from the recipient.

Unsolicited emails can only be sent without consent if:

- The contact details were provided in the course of a sale;
- The marketing relates to a similar product; and
- The recipient was given a method to opt-out of the use of their contact details for marketing when they were collected.

In addition, the Law also prohibits the use of automated calling systems without the consent of the recipient.

Direct marketing emails may not disguise or conceal the identity of the sender. SMS marketing is also likely to be included within this prohibition on email marketing.

The restrictions on marketing by email only apply to email marketing sent to individuals and not to email marketing sent to corporations.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The Law does not specifically address the collection of location and traffic data by public electronic communications services providers, or the use of cookies (or similar technologies).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

37. NETHERLANDS

CONTRIBUTION DETAILS

Richard van Schaik
Partner
T +31 20 5419828
richard.vanschaik@dlapiper.com

Prof. Jan Kabel
Of Counsel
T +31 20 5419312
jan.kabel@dlapiper.com

LAW

The Netherlands implemented the EU Data Protection Directive 95/46/EC on 1 September 2001 with the Dutch Personal Data Protection Act ("**Wbp**"). Enforcement is through the Dutch Data Protection Authority ("**College Bescherming Persoonsgegevens**").

DEFINITION OF PERSONAL DATA

Any data relating to an identified or identifiable natural person.

DEFINITION OF SENSITIVE PERSONAL DATA

Personal data regarding a person's religion or philosophy of life, race, political persuasion, health and sexual life, trade union membership, criminal behaviour and personal data regarding unlawful or objectionable conduct connected with a ban imposed as a result of such conduct.

NATIONAL DATA PROTECTION AUTHORITY

The College Bescherming Persoonsgegevens
Juliana van Stolberglaan 4-10
2595 CL DEN HAAG
Postbox 93374
2509 AJ DEN HAAG
T 00.31.70 – 8888 500
F 00.31.70 – 8888 501
www.cbpweb.nl

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

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

The notification shall, *inter alia*, include the following information:

- name and address of the data controller;
- purpose(s) of the processing;
- data subjects or categories of data subjects;
- data or categories of data relating to these data subjects;
- recipients or categories of recipients;
- proposed transfers of personal data to countries outside the European Union; and
- a general description of the security measures the data controllers is planning to take.

If any of the following changes occurs, the data controller must notify the College Bescherming Persoonsgegevens of these changes within one year after the previous notification. This concerns changes in:

- the purpose or purposes of the data processing;
- the data subjects and recipients or categories of data subjects and recipients;
- the security measures; and/or
- the intended transfers to countries outside the European Union.

However, this is only required if the changes are not of a purely incidental nature.

Also, any change to the name or address of the data controller should be notified to the College Bescherming Persoonsgegevens within one week.

DATA PROTECTION OFFICERS

Companies, industry associations, governments and institutions can appoint a data protection officer. There is no legal requirement in the Netherlands to do so. The data protection officer ensures that processing of personal data will take place in accordance with the Wbp. The statutory duties and powers of the data protection officer gives this officer an independent position within the organization.

COLLECTION AND PROCESSING

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

For collecting personal data:

Pursuant to the Wbp, a data controller may only collect personal data if he has a purpose for this.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The purpose must be:

- specified;
- explicit; and
- legitimate.

A data controller may not collect data if he has not clearly specified the purpose.

For processing personal data:

- the data subject has unambiguously given his prior consent thereto;
- the processing is necessary for the performance of a contract to which the data subject is party;
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is necessary or legally required in order to protect an important public interest; or
- the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data is supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

In addition, personal data may not be further processed in a way incompatible with the purposes the data was collected. Whether further processing is incompatible depends on different circumstances, such as:

- the relationship between the purpose of the intended processing and the purposes for which the data originally was obtained;
- the nature of the data concerned;
- the consequences of the intended processing for the data subject;
- the manner in which the data have been obtained; and
- the extent to which appropriate guarantees have been put in place with respect to the data subject.

Also, personal data may only be processed, where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive.

Finally, the Wbp sets out strict rules in relation to sensitive data. The main rule is that such data may not be processed, unless the data subject has given its explicit consent to it.

TRANSFER

Transfer of a data subject's personal data to non EU/European Economic Area countries is allowed if the countries provide "adequate protection". For transfer of data to the United States, companies which adhere to the US/EU Safe Harbor principles are deemed to offer adequate protection.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

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

- the data subject has unambiguously given its consent thereto;
- the transfer is necessary for the performance of the contract between the data controller and the data subject;
- the transfer is necessary in respect of an important public interest, or for the establishment, exercise or defence in law of any right;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer occurred from a register that was set by law and can be consulted by anyone or by any person demonstrating a legitimate interest;
- the transfer is based on unchanged Model Clauses as referred to in article 26(4) of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; or
- a permit thereto has been granted by Minster of Justice, after consultation of the College Bescherming Persoonsgegevens. In order to obtain such permit, certain conditions should be met. One of these conditions can be implementing Binding Corporate Rules (BCR).

BCR are internal codes of conduct regarding data privacy and security, to ensure that transfers of personal data outside the European Union will take place in accordance with the EU rules on data protection.

The use of BCRs is not obligatory. It will however bring benefits to both processors and controllers.

Once BCRs are approved they can be used by the controller and processor, thereby ensuring compliance with the EU data protection rules without having to negotiate the safeguards and conditions each and every time a contract is entered into.

SECURITY

Data controllers and processors must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

BREACH NOTIFICATION

The Wbp does not yet provide for a data security breach notification duty.

MANDATORY BREACH NOTIFICATION

There is no mandatory requirement in the Wbp. However, a legislative bill introduces the obligation to report such a data breach as soon as possible to the College Bescherming Persoonsgegevens. If a data breach is not reported, the College Bescherming Persoonsgegevens can impose a fine up to EUR 200,000.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

In case of possible violations of the Wbp, the College Bescherming Persoonsgegevens can impose the following sanctions:

- Enforce an administrative order. The data controller would be forced to change its policy with immediate effect;
- Administrative fines up to a maximum of EUR 19,500 may be imposed by the Authority in case of violation of the notification duty; or
- Penal sanctions could be punished with a fine of the second category in case of contravention of:
  - the duty to designate a person or body in the Netherlands to act on party who are not established in the European Union, but make use of means situated in the Netherlands;
  - the notification duties mentioned before;
  - transfer of personal data to a country outside the European Union that is not considered to guarantee an adequate level of protection, or transfer without permit to those countries.

ELECTRONIC MARKETING

Electronic marketing is partially regulated in Article 11.7 of the Dutch Telecommunications Act. In the context of this Article electronic marketing could be defined as SMS, e-mail, fax and similar media for the purposes of unsolicited communication related to commercial, charitable or ideal purposes without the individuals' prior express consent.

Electronic marketing directed to corporations does not require prior consent if:

- the advertiser/electronic marketer uses electronic address data which are meant to be for this particular purpose;
- if the individual is located outside the EU, the advertiser/electronic marketer complies with the relevant rules of that particular country in this respect.

On the basis of Article 11.7 electronic marketing to individuals is in principle prohibited. If certain conditions are being met, such as prior express consent, electronic marketing directly to individuals can be allowed. Furthermore, electronic marketing to individuals is also allowed if it is restricted to the marketing of existing customers and restricted to similar products/services of the advertiser/electronic marketer. In the last case, the advertiser/electronic marketer is obliged to provide opt-out possibilities to his customers when obtaining the data from the customers and in every marketing message sent.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Traffic Data – Traffic Data is regulated in Article 11.5 of the Dutch Telecommunications Act. Traffic Data held by a public electronic communications services provider ("**CSP**") must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service; and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- The management of billing or traffic;
- Dealing with customer enquiries;
- The prevention of fraud;
- The provision of a value added service (subject to consent); or
- Market research (subject to consent).

Location Data (Traffic Data not included) – Location Data is regulated in Article 11.5a of the Dutch Telecommunications Act.

Location Data may only be processed:

- If these data are being processed in anonymous form; or
- With informed consent of the individual.

Cookie Compliance – The amended E Privacy Directive requires the user to consent to the use of cookies. On 5 June 2012, the Netherlands implemented the E-Privacy Directive through the Dutch Telecommunications Act in Article 11.7a. (hereinafter: Article 11.7a). The Independent Post and Telecommunications Authority ("**OPTA**") is entrusted with the enforcement of Article 11.7a.

The main rule is that the website operator needs to obtain prior consent from a user before using cookies (opt-in). It is necessary to obtain the informed agreement of website visitors to the use of cookies by way of an "I agree" button or a similar arrangement. Implicit consent is not sufficient under Dutch law. Please note that the website operator is entitled to refuse website visitors access to its website(s) if no consent is given.

The requirement to obtain prior consent from a user does not apply where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user. An example is that of where a user of a site has chosen the goods they wish to buy and the user clicks the "add to basket" or "proceed to checkout" button, the site remembers what they have chosen from the previous page. This cookie is deemed "strictly necessary" to provide the service requested by the user, therefore no consent to the storage of such a cookie is required.

As per 1 January 2013, the information collected through cookies are to be considered 'personal data', unless the party which places the cookies can prove otherwise. This goes only for tracking cookies, whereby the surfing behaviour of customers on several different websites is being observed (and the information obtained is being used for commercial purposes).

In case of violation of electronic marketing or online privacy legislation, the OPTA can impose fines up to EUR 450,000 per violation.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

39. NEW ZEALAND

CONTRIBUTION DETAILS

Brian Bray
Partner
T +64 4 474 3236
M +64 27 255 5700
brian.bray@dlapf.com

LAW

The Privacy Act 1993 ("Act") governs how agencies collect, use, disclose, store and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities or types of personal information. Codes in place as at 31 January 2013 are:

- Credit Reporting Privacy Code;
- Health Information Privacy Code;
- Justice Sector Unique Identifier Code;
- Superannuation Schemes Unique Identifier Code;
- Telecommunications Information Privacy Code; and
- Civil Defence National Emergencies (Information Sharing) Code.

Enforcement is through the Privacy Commissioner.

DEFINITION OF AGENCY

"*Agency*" is defined under the Act as any person or body of persons, whether corporate or unincorporated, and whether in the public sector (including a government departments) or the private sector. Certain bodies are specifically excluded from the definition.

DEFINITION OF PERSONAL DATA

Personal data is "*Personal information*" under the Act and defined as information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

No differentiation is made between how different types of personal information are to be treated under the Act.

NATIONAL DATA PROTECTION AUTHORITY

The Privacy Commissioner's Office
Level 4
109-111 Featherston Street
Wellington 6143
New Zealand
T +64 474 7590
F +64 474 7595
enquiries@privacy.org.nz
www.privacy.org.nz

REGISTRATION

There is no obligation on agencies to notify the Privacy Commissioner that they are processing personal information. However, the Privacy Commissioner may require an agency to supply information for the purpose of publishing or supplementing a directory or to enable the Commissioner to respond to public enquiries in this regard.

The Privacy Commissioner may from time to time publish a directory of personal information including:

- The nature of any personal information held by an agency;
- The purpose for which personal information is held by an agency;
- The classes of individuals about whom personal information is held by an agency;
- The period for which personal information is held by an agency;
- The individuals entitled to access personal information held by an agency and the conditions relating to such access; and
- Steps to be taken by an individual wishing to obtain access to personal information held by an agency.

DATA PROTECTION OFFICERS

The Act requires all agencies to appoint a privacy officer. The privacy officer's responsibilities include:

- The encouragement of compliance with personal information privacy principles;
- Dealing with requests made to the agency pursuant to the Act;
- Working with the Privacy Commissioner in relation to investigations relating to the agency; and
- Ensuring compliance with the provisions of the Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

Subject to specific exceptions, agencies may collect, store and process personal data in accordance with any of the following 12 "Privacy Principles":

1. The personal information is needed for a lawful purpose connected with the agency's work;
2. The personal information is collected directly from the relevant person;
3. Before the information is collected, the agency has taken reasonable steps to ensure that the person knows that the information is being collected; the purpose for which it is being collected; the intended recipients; the name and address of the agency collecting and holding the information; if the information is authorised or required by law, the applicable law and the consequences if the requested information is not provided; and that the person concerned may access and correct the personal information;
4. The personal information is not collected in an unlawful or unfair way or in a way that unreasonably invades a person's privacy;
5. The personal information must be kept reasonably safe from being lost, accessed, used, modified or disclosed to unauthorised persons;
6. If the personal information is easily accessible, the relevant person is entitled to know whether information is held and to have access to it;
7. Where an agency holds personal information, the relevant person is entitled to request correction of the information. If the agency will not correct the information, the person may provide a statement of the correction sought to be attached to the personal information;
8. Before it is used, the agency must check the personal information is accurate, up to date, complete, relevant and not misleading;
9. The personal information may not be kept for any longer than it is needed;
10. Subject to certain exceptions, personal information collected for one purpose may not be used for another purpose;
11. An agency must not disclose personal information to another person, body or agency except in specific circumstances; and
12. An agency may only assign a unique identifier to an individual if it is needed for the agency to carry on its work efficiently and may not assign a unique identifier to an individual if the same identifier is used by another agency.

Personal information does not need to be collected directly from the relevant person if:

- The personal information is publicly available.
- The relevant person authorises collection of the personal information from someone else.
- Non-compliance would not prejudice the interests of the relevant individual.
- The personal information is being collected for a criminal investigation, enforcement of a financial penalty, protection of public revenue or the conduct of court proceedings.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Compliance would prejudice the purpose of the collection of the personal information or is not practical in the circumstances.
- The personal information will be used in a way which will not identify the person concerned.

TRANSFER

An agency should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country ("**State**") by issuing a transfer prohibition notice ("**Notice**") if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines, which include:

- The collection limitation principle (there should be limits to the collection of personal data);
- The data quality principle (personal data should be accurate, complete and kept up to date);
- The purpose specification principle (the purposes for which personal data are collected should be specified);
- The use limitation principle (personal data should not be used otherwise than in accordance with the purpose specification principle, except with the consent of the data subject or by authority of law);
- The security safeguards principle (personal data should be protected by reasonable security safeguards);
- The openness principle (there should be a general policy of openness about developments, practices and policies relating to personal data);
- The individual participation principle (individuals should have the right to obtain confirmation of whether a data controller holds their personal data, to have that data communicated to him/her, to be given reasons if a request for that data is denied and to be able to challenge that denial, and to challenge data relating to him/her and have that data erased, rectified, completed or amended if successful); and
- The accountability principle (a data controller should be accountable for complying with the above principles).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

In considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information between New Zealand and other States, and any existing or developing international guidelines relevant to trans border data flows.

On 19 December 2012 the European Commission issued a decision formally declaring that New Zealand law provides a standard of data protection that is adequate for the purposes of EU law. This decision means that personal data can flow from the 27 EU member states to New Zealand for processing without any further safeguards being necessary.

SECURITY

An agency that holds personal information shall ensure that the information is kept securely and protected by such security safeguards as are reasonable in the circumstances to protect against:

- loss;
- access, use, modification or disclosure, except with the authority of the agency; and
- other misuse or unauthorised disclosure.

If it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency must be done to prevent unauthorised use or unauthorised disclosure of the information.

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report an interference with privacy.

Any person may make a complaint to the Privacy Commissioner alleging an action is, or appears to be, an interference with the privacy of an individual. For there to be an interference with privacy, there must be a breach of the law and the breach must lead to financial loss or other injury, an adverse effect on a person's right, benefit, privilege, obligation or interest or significant humiliation, loss of dignity or injury to a person's feelings. There is no requirement to show harm in a complaint about access to, or correction of, personal information. An unauthorised disclosure of personal information is sufficient to breach the Act.

ENFORCEMENT

In New Zealand, the Privacy Commissioner is responsible for investigating a breach of privacy laws. The Privacy Commissioner has powers to enquire into any matter if she believes that the privacy of an individual is being, or is likely to be, infringed. The Privacy Commissioner will primarily seek to settle a complaint by conciliation and mediation. If a complaint cannot be settled in this way, a formal investigation may be conducted so that the Privacy Commissioner may form an opinion on how the law applies to the complaint. The Privacy Commissioner's opinion is not legally binding but is highly persuasive. The Privacy Commissioner is not able to issue a formal ruling or determination and cannot begin prosecution proceedings or impose a fine.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

If the Privacy Commissioner is of the opinion that there has been an interference with privacy, she may refer the matter to the Director of Human Rights who may then in turn decide to take the complaint to the Human Rights Review Tribunal. The Tribunal will hear the complaint afresh and its decision is legally binding.

ELECTRONIC MARKETING

The Act does not differentiate between the collection of and use of any 'personal information' for electronic marketing or other forms of direct marketing.

The Unsolicited Electronic Messages Act 2007:

- prohibits unsolicited commercial electronic messages (this includes email, fax, instant messaging, mobile/smart phone text (TXT) and image-based messages of a commercial nature – but does not cover internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand).
- requires commercial electronic messages to include accurate information about who authorised the message to be sent;
- requires a functional unsubscribe facility to be included so that the recipient can instruct the sender not to send the recipient further messages; and
- prohibits using address-harvesting software to create address lists for sending unsolicited commercial electronic messages.

The Marketing Association of New Zealand has a Code of Practice for direct marketing which governs compliance by members of the principles of the code. The Code establishes a "Do Not Call" register to which anyone not wanting to receive any direct marketing can register.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Other than compliance with the Act, no additional legislation deals with the collection of location and traffic data by public electronic communications services providers and use of cookies (and similar technologies). The New Zealand Privacy Commissioner has general guidelines on protecting online privacy.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

40. NORWAY

CONTRIBUTION DETAILS

Nils Arne Grønlie
Partner
T +47 41916542
nils.arne.gronlie@dlaiper.com

LAW

A contracting party to the European Economic Area ("**EEA**") Agreement, Norway implemented the EU Data Protection Directive 95/46/EC in April 2000 with the Personal Data Act 2000 ("**Act**"). Enforcement is through the Data Protection Authority ("**DPA**").

DEFINITION OF PERSONAL DATA

Any information and assessments that may be linked to a natural person (the Act section 2, number 1).

DEFINITION OF SENSITIVE PERSONAL DATA

Information relating to a) racial or ethnic origin, or political opinions, philosophical or religious beliefs, b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, c) health, d) sex life, or e) trade union membership (the Act section 8).

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Agency
Nw: Datatilsynet
P.O. Box 8177 Dep, N-0034 Oslo
T +47 22 39 69 00
T +47 22 42 23 50
F +47 22 42 23 50
www.datatilsynet.no

REGISTRATION

Unless an exemption applies, data controllers who process personal data by automatic means must notify the DPA so that their processing of personal data may be registered and made public. Changes to the processing of personal data will require the notification to be amended and a new notification shall in any event be given three years after the previous notification was given.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The notification shall, inter alia, include the following information (as outlined in the DPA's standard electronic notification form):

- the purpose(s) of the processing;
- the controller's contact details and sector;
- whether sensitive personal data are processed;
- whether a data processor processes data on behalf of the controller; and
- whether the data will be transferred outside the EEA.

DATA PROTECTION OFFICERS

There is no requirement in Norway for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

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

- the data subject consents;
- there is statutory authority for the processing;
- the processing is necessary to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract;
- the processing is necessary to enable the controller to fulfil a legal obligation;
- the processing is necessary to protect the vital interests of the data subject;
- the processing is necessary to perform a task in the public interest;
- the processing is necessary to exercise official authority, or
- the processing is necessary to enable the controller or third parties to whom the data is disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject.

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of additional conditions.

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies. The notification shall include information on the identity of the controller, the purposes of the processing, whether the data will be disclosed and if so, the identity of the controller, the fact that the provision of data is voluntary and any other circumstances that will enable the data subject to exercise his rights pursuant to the Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

Data controllers may transfer personal data out of the EEA if any of the following conditions are met:

- the data subject has consented to the transfer;
- there is an obligation to transfer the data pursuant to an international agreement or as a result of membership of an international organisation;
- the transfer is necessary for the performance of a contract with the data subject, or for the performance of tasks at the request of the data subject prior to entering into such a contract;
- the transfer is necessary for the conclusion or performance of a contract with a third party in the interest of the data subject;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is necessary on order to establish, exercise or defend a legal claim; or
- the transfer is necessary or legally required in order to protect an important public interest, or there is statutory authority for demanding data from a public register.

The DPA may allow transfers even if the above conditions are not fulfilled if the data controller provides adequate safeguards with respect to the protection of the rights of the data subject.

Transfer of a data subject's personal data to non EU/EEA countries is allowed if the countries provide adequate protection for the security of the data, or if the transfer is covered by standard contractual clauses approved by the European Commission, or subject to an organisation's Binding Corporate Rules. Countries which have implemented Directive 95/46/EC meet the requirement as regards an adequate level of protection.

Transferors are required to seek permission from the DPA for any transfers of personal data; (i) not based on the conditions above; (ii) to countries outside the EEA; or which do not have an adequate protection level; or (iii) to entities (outside the jurisdictions mentioned in (ii)) which do not have Binding Corporate Rules or are not a member of the US Safe Harbor scheme. (the Act section 30 second paragraph).

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of Norway's transfer law.

SECURITY

Data controllers and processors shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data.

BREACH NOTIFICATION

Data security breaches which have resulted in the unauthorised disclosure of personal data where confidentiality is necessary, is subject to notification to the DPA. DPA guidance and practice indicates that data subjects may need to be notified provided the discrepancy may be detrimental to the interests of the data subject (eg identity theft, forgery, harassment).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

The DPA is responsible for enforcement of the Act, and DPA's decisions may be appealed to the Privacy Appeals Board (Nw: Personvernnemnda). If the DPA becomes aware that a data controller is in breach of the Act, it may issue an order requiring the controller to rectify the position. In connection with orders, the DPA may impose a coercive fine which will run for each day from the expiry of the time limit set for compliance with the order until the order has been complied with.

Failure to comply with an order is a criminal offence and may be punished with fines or imprisonment.

The DPA may also issue fines (Data Offence Fines) up to a maximum of 10 times the National Insurance Basic Amount (approx. EUR 90,000). Physical persons may only be fined for a data offence for deliberate or negligent violation. A business may not be fined for a data offence for a violation that is due to factors outside the control of the business. In evaluating whether to impose a data offence fine and in determining its size, special consideration will be given to:

- how seriously the violation has infringed the interests the Act is designed to protect;
- the degree of culpability;
- whether the violator could, by guidelines, instructions, training, inspection or other measures, have mitigated the violation;
- whether the violation was committed to promote the violators interests;
- whether the violator has, or could have, achieved any benefit from the violation;
- whether this is a repeat violation;
- whether other sanctions following from the violation are imposed on the violator, or a person acting on his behalf, for instance punishment of a person for a criminal offence, and
- the violator's financial capacity.

The controller shall compensate damage suffered as a result of the fact that personal data have been processed contrary to the provisions of the Act, unless the damage is not due to error or neglect on the part of the controller.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be "personal data" for the purposes of the Act).

Pursuant to the Marketing Control Act (Nw: Markedsføringsloven) section 15, it is prohibited in the course of trade, without the prior consent of the recipient, to send marketing communications to natural persons using electronic methods of communication which permit individual communication, such as electronic mail, telefax or automated calling systems (calling machines).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Prior consent is however not required for electronic mail marketing where there is an existing customer relationship and the contracting trader has obtained the electronic address of the customer in connection with a sale. The marketing may only relate to the trader's own goods, services or other products corresponding to those on which the customer relationship is based.

At the time that the electronic address is obtained, and at the time of any subsequent marketing communication, the customer shall be given a simple and free opportunity to opt out of receiving such communications.

"Electronic mail" in the context of the Marketing Control Act means any communication in the form of text, speech, sound or image that is sent via an electronic communications network, and that can be stored on the network or in the terminal equipment of the recipient until the recipient retrieves it. This includes text and multimedia messages sent to mobile telephones.

Direct marketing emails must not conceal or disguise the identity of the sender. If the email is unsolicited, it shall clearly state that the email contains a marketing message. upon reception of the message (The Norwegian E-commerce Act, Nw: Ehandelsloven, section 9).

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Traffic Data – Traffic data is defined in Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services (Nw: Ekomforskriften F16.02.2004 nr 401) section 7-1 as data which is necessary to transfer communication in an electronic communications network or for billing of such transfer services.

Processing of traffic data held by a Communications Services Provider ("CSP") (Nw: Tilbyder) may only be performed by individuals tasked with invoicing, traffic management, customer enquiries, marketing of electronic communications networks or the prevention or detection of fraud.

Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication (Electronic Communications Act section 2-7 (Nw: Ekomloven). However, Traffic Data can be retained if it is being used to provide a value added service and consent has been given for the retention of the Traffic Data.

Location Data – Location data may only be processed subject to explicit consent for the provision of a value added service which is not a public telephony service, and the users must be given understandable information on which data is processed and how the data is used. The user shall have the opportunity to withdraw her consent. See Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services section 7-2.

Cookie Compliance – The Norwegian Regulation relating to Electronic Communications Networks and Electronic Communications Services section § 7-3, requires that information about the use of cookies is provided to the users in accordance with the Act, including the purpose of the processing and that they are given an opportunity to object to the processing, i.e. opt-out.

Regardless of this, the use of cookies for technical storage or access to information is allowed if this is done solely for the purpose of transferring or easing the transfer of communication, or if this is necessary to provide an information society service pursuant to the user's explicit consent. The amended E-Privacy Directive, requiring opt-in for cookies, has not been implemented into Norwegian law yet albeit there is a proposed amendment currently in process. The proposed amendment to Norwegian law seems to be in line with the amended E-Privacy Directive.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

41. PAKISTAN

CONTRIBUTION DETAILS

Liaquat Merchant Associates
Barristers-at-law,
Advocates & Corporate Legal Consultants
4C, 9th Commercial Lane
Zamzama Boulevard, Phase V, DHA
Karachi – Pakistan
T +9221 3583 5101 – 104
www.liaquatmerchant.com

Darakhshan Sheikh Vohra
Partner
d.vohra@liaquatmerchant.com

Saqiba Akhlaq Khan
Associate
s.akhlaq@liaquatmerchant.com

LAW

There is, at the date of publication, no legislation regulating the protection of data in Pakistan. A draft Electronic Data Protection Bill, limited to protection of electronic data was circulated by the Ministry of Information in 2005.

DEFINITION OF PERSONAL DATA

In the absence of any legislation regulating the protection of data in Pakistan, the term "personal data" is undefined.

DEFINITION OF SENSITIVE PERSONAL DATA

In the absence of any legislation regulating the protection of data in Pakistan, the term "sensitive personal data" is undefined.

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in Pakistan.

REGISTRATION

Data controllers or collectors do not need to register with any authority.

DATA PROTECTION OFFICERS

Organisations in Pakistan are not required to appoint a data protection officer.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

Data controllers can collect and process personal data under any conditions.

TRANSFER

Although the transfer of data to third parties is not specifically regulated under the laws of Pakistan, data cannot be transferred from Pakistan to a country which is not recognised by Pakistan. Pakistan currently does not recognize Israel, Taiwan, Kosovo, Somaliland, Nagorno Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Furthermore, data can only be transferred to India if such a transfer can be justified by the transferor.

Besides being regulated by contractual terms, data collated by, inter alia, banks, insurance firms, hospitals, defence establishments and other "sensitive" installations/institutions cannot be transferred to any individual/body unless it is transferred with the permission of the relevant regulator or similar bodies on a confidential basis. Additionally, in certain cases data cannot be transferred without the permission of the relevant client/customer.

SECURITY

Data controllers do not have to fulfil any security requirements.

BREACH NOTIFICATION

Data security breaches or losses do not have to be reported or notified to anybody or individual.

ENFORCEMENT

In the absence of any legislation in the sphere of data protection no body or entity enforces any law. Enforcement and appropriate relief may however be sought through courts of law having jurisdiction in the matter.

ELECTRONIC MARKETING

There is, at the date of publication, no legislation regulating electronic marketing in Pakistan. Please note that an earlier law promulgated in this regard has since lapsed. A draft Prevention of Electronic Crimes Bill which may potentially deal with electronic marketing is currently under consideration of a select committee of the National Assembly. This draft law is more wide ranging in nature than its predecessor.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is, at the date of publication, no legislation regulating online privacy in Pakistan. Please note that an earlier law promulgated in this regard has since lapsed. A draft Prevention of Electronic Crimes Bill which may potentially deal with online privacy is currently under consideration of a select committee of the National Assembly. This draft law is more wide ranging in nature than its predecessor.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

42. PANAMA

CONTRIBUTION DETAILS

Galindo, Arias & Lopez
Federico Boyd Ave. No.18 and 51st Street
Scotia Plaza, 11th Floor
P.O. Box 0816-03356
Panama, Republic of Panama
www.gala.com.pa

Diego Herrera
T +507 303 0303
D +507 303 0339
F +507 303 0434
dherrera@gala.com.pa

James Sattin
T +507 303 0303
D +507 303 0453
F +507 303 0434 |
jsattin@gala.com.pa

Jose Luis Sosa
T +507 303 0303
D +507 303 0323
F +507 303 0434
jsosa@gala.com.pa
eileen.batac@romulo.com

LAW

In recent years, Panama has taken significant legislative steps to regulate electronic data protection and internet commerce. However, this regime remains a work in progress.
The primary laws and regulations thus far enacted are Law 51 of 22 July 2008, as amended by Law 82 of 9 November 2012 ("**Law 51**"), and Executive Decree No. 40 of 19 May 2009 ("**Decree 40**"). The central purpose of both Law 51 and Decree 40 is to regulate the creation, utilization and storage of electronic documents and signatures in Panama, through a registration process and the supervision of providers of data storage services. Law 51 and Decree 40 provide for enforcement through the General Directorate of Electronic Commerce (*Dirección General de Comercio Electrónico*) ("**DGCE**").

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF PERSONAL DATA

Personal Data is not expressly defined under Panamanian law. However, it is generally deemed to include information that can specifically identify an individual, such as one's name, postal address (including billing and shipping addresses), telephone number, e-mail address, credit card number, or a username.

DEFINITION OF SENSITIVE PERSONAL DATA

"Sensitive Personal Data" is not defined under Panamanian Law.

NATIONAL DATA PROTECTION AUTHORITY

The General Directorate of Electronic Commerce
(Dirección General de Comercio Electrónico)
Plaza Edison, Sector El Paical, Floors 2 & 3.
T (507) 560-0600; (507) 560-0700
F (507) 261-1942
contactenos@mici.gob.pa

REGISTRATION

Under Decree 40, electronic data storage companies and companies engaged in online electronic signature verification must register with the DGCE. For companies otherwise engaged in e-commerce-related activities, registration with the DGCE is voluntary and can be completed online and free of cost. Registration must occur no later than 15 days prior to the commencement of data processing activities and shall include, *inter alia*, the following information:

- name of the company;
- company´s physical address, telephone and fax number;
- legal representative of the company;
- company´s internet address or URL;
- contact email provided by company to customers;
- public Registry and Ministry of Commerce Registration Information;
- in the event that an undertaken activity requires specific authorization or permits, evidence thereof;
- tax Identification Number;
- description of services offered by the company, including pricing information and applicable taxes; and
- the Company's code of conduct.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Moreover, for companies that are engaged in each of the activities for which registration is mandatory, Law 51 and Decree 40 set forth certain additional registration requirements.

DATA PROTECTION OFFICERS

Appointment of a data protection officer is not required.

COLLECTION AND PROCESSING

In Panama, personal information is protected at the constitutional level. The Constitution provides that any person or entity that obtains personal information and/or personal documents, either from a person or a company who provides such information willingly, or through any other means, may not disclose such information without the consent of its lawful owner (there is no specific definition or explanation of who is considered the "lawful owner" of personal information). An exception to the consent rule is the disclosure of such information pursuant to a valid judicial or governmental request.

The disclosure of personal information without consent is also prohibited by the Panamanian Criminal Code. Criminal penalties apply to the disclosure of personal information when the disclosure causes harm to the information's lawful owner. Law 51 specifically establishes that this criminal law prohibition applies to electronically stored information.

Panamanian law further requires that providers of online data storage services take reasonable measures to ensure that company personnel who come into contact with confidential information do not have a criminal record, have obtained the necessary technical skills to handle such data and information, and possess reasonable knowledge of existing legal restrictions related to the disclosure of such information. Although this prohibition is specifically intended to apply to entities that provide online data storage services, it is not unforeseeable that it could also be construed to apply to any company engaged in e-commerce.

TRANSFER

Although the Panamanian e-commerce regulatory framework is not yet fully developed, the existing regulations follow the constitutional principle that the consent of the lawful owner is required for the transfer of any personal information.

Pursuant to Law 51, when a customer provides his email address during the process of acquiring or subscribing to a service offered online, the company providing such service must disclose to the customer its intent to use the email address in the future for commercial communications and, further, must obtain the customer's express consent for such purposes. The client or customer must also be able to revoke such consent easily, through a simple process made available by the provider of the service.

While the manner in which this restriction appears to have been drafted suggests that it applies exclusively to online service providers, its broader application to all companies that sell products online or are engaged in e-commerce activities is foreseeable.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Decree 40 establishes certain security requirements applicable only to electronic data storage and electronic signature verification companies, for whom registration with the DGCE is mandatory. The main requirements are adherence to the security parameters periodically published by the DGCE, and the performance of annual self-audits, the results of which must be filed with the DGCE in order for the company to renew its registration. In addition, these companies must create a disaster recovery plan that allows such providers to re-establish regular operations within twelve hours of the occurrence of a disruptive event.

No similar provisions have been enacted with respect to companies who engage in other types of e-commerce, ie, those for whom registration is voluntary.

BREACH NOTIFICATION

Law 51 does not require breach notification.

ENFORCEMENT

The DGCE is responsible for enforcement of the existing e-commerce and related regulations, including the publication of additional complementary regulations. Sanctions include the suspension or permanent ban of the activities of companies that infringe certain regulations, as well as fines of up to US$150,000.

ELECTRONIC MARKETING

With respect to email advertising, Panamanian law requires that all such emails: (i) state that they are commercial communications; (ii) include the name of the sender; and (iii) set forth the mechanism through which the recipient may choose not to receive any further communications from the particular sender. These requirements apply to other promotional offers as well.

Further, although opt-out tools are not prohibited, the client's initial opt-in consent is specifically required to use the client's email for advertising purposes. Further, although no specific prohibition has been enacted with respect to the use of information for online advertising, obtaining the customer's consent is always preferable.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The existing regulatory framework does not yet address location data, cookies, local storage objects or other similar data-gathering tools.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

43. PHILIPPINES

CONTRIBUTION DETAILS

Romulo Mabanta Buenaventura Sayoc & De Los Angeles
21st Floor, Philamlife Tower
8741 Paseo De Roxas
Makati City, Metro Manila
Philippines
www.romulo.com

Eileen Rosario Cordero-Batac
Partner
T +63 2 555 9555
eileen.batac@romulo.com

Catherine O. King Kay
Paralegal
T +63 2 555 9555
catherine.kingkay@romulo.com

LAW

The Philippines recently enacted the Data Privacy Act of 2012 (the "**Act**") or Republic Act No. 10173, which took effect on 8 September 2012.

DEFINITION OF PERSONAL DATA

Personal Information is defined in the Act as "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."

The Act, in addition to defining "Personal Information" that is covered by the law, also expressly excludes certain information from its coverage. These are:

- Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
  - The fact that the individual is or was an officer or employee of the government institution;
  - The title, business address and office telephone number of the individual;
  - The classification, salary range and responsibilities of the position held by the individual; and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

  - The name of the individual on a document prepared by the individual in the course of employment with the government;
- Information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;
- Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;
- Personal information processed for journalistic, artistic, literary or research purposes;
- Information necessary in order to carry out the functions of a public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
- Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Philipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and
- Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive Personal Information is defined in the Act as personal information:

- About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
- Specifically established by an executive order or an act of Congress to be kept classified.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The Act provides for the creation of a National Privacy Commission. As of 15 January 2013, the National Privacy Commission has not been constituted.

REGISTRATION

There is no system of mandatory registration provided in the Act.

DATA PROTECTION OFFICERS

The Personal Information Controller of an organisation must appoint a person or persons who shall be accountable for the organisation's compliance with the Act, and the identity of such person or persons must be disclosed to the data subjects upon the latter's request.

COLLECTION AND PROCESSING

The collection and processing of Personal Information must comply with the general principle that Personal Information must be:

- Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
- Processed fairly and lawfully;
- Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
- Adequate and not excessive in relation to the purposes for which they are collected and processed;
- Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or 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: Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, that adequate safeguards are guaranteed by said laws authorizing their processing.

In addition, the processing of personal information must meet the following criteria, otherwise, such processing becomes prohibited:

- The data subject has given his or her consent;
- The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- The processing is necessary to protect vitally important interests of the data subject, including life and health;
- The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
- The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

The processing of sensitive personal information is prohibited, except in the following cases;

- The data subject has given his or her specific consent prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- The processing is provided for by existing laws and regulations, provided that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information, and the consent of the data subjects is not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
- The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations, provided, (i) such processing is only confined and related to the bona fide members of these organizations or their associations, (ii) the sensitive personal data are not transferred to third parties, and (iii) the consent of the data subject was obtained prior to processing;
- The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
- The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

The transfer of Personal Information is permitted without any restrictions or prerequisites, but the Personal Information Controller remains responsible for personal information under its control or custody that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. The transfer, however, of sensitive personal information to third parties is prohibited.

SECURITY

The personal information controller must implement reasonable and appropriate organisational, physical and technical measures to protect personal information against any type of accidental or unlawful destruction, such as from accidental loss, unlawful access, fraudulent misuse, unlawful destruction, alteration, contamination and disclosure, as well as against any other unlawful processing.

The determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.

In addition, the security measures to be implemented must include the following, which are subject to guidelines that the National Privacy Commission may issue:

- safeguards to protect its computer network against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability;
- a security policy with respect to the processing of personal information;
- a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
- regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

The personal information controller is obligated to ensure that third parties processing personal information on its behalf shall implement the security measures required by the Act.

The obligation to maintain strict confidentiality of personal information that are not intended for public disclosure extends to the employees, agents or representatives of a personal information controller who are involved in the processing of such personal information.

BREACH NOTIFICATION

The Personal Information Controller is required to promptly notify the National Privacy Commission and the affected data subjects when it has reasonable belief that sensitive personal information or other information has been acquired by an unauthorised person, and that (a) such personal information may, under the circumstances, be used to enable identity fraud and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

(b) the Personal Information Controller or the National Privacy Commission believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach.

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The National Privacy Commission may also authorize postponement of notification where such notification may hinder the progress of a criminal investigation related to a serious breach.

Notification is not required if the National Privacy Commission determines (a) that notification is unwarranted after taking into account compliance by the Personal Information Controller with the Act and the existence of good faith in the acquisition of personal information, or (b) in the reasonable judgment of the National Privacy Commission, such notification would not be in the public interest or in the interests of the affected data subjects.

ENFORCEMENT

The National Privacy Commission is responsible for ensuring compliance of the Personal Information Controller with the Act. It has the power to receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report. Additionally, the National Privacy Commission can issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest.

The National Privacy Commission, however, cannot prosecute violators for breach of the Act for which criminal penalties can be imposed. The Department of Justice is tasked with the prosecution for violations of the Act that are punishable with criminal sanctions.

The following actions are punishable by the Act with imprisonment in varying duration plus a monetary penalty:

- Processing of personal information or sensitive personal information; (i) without the consent of the data subject or without being authorised by the Act or any existing law; or (ii) for purposes not authorised by the data subject or otherwise authorised under the Act or under existing laws;
- Providing access to personal information or sensitive personal information due to negligence and without being authorised under this Act or any existing law;
- Knowingly or negligently disposing, discarding or abandoning the personal information or sensitive personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Knowingly and unlawfully, or violating data confidentiality and security data systems, breaking in any way into any system where personal and sensitive personal information is stored;
- Concealing the fact of such security breach, whether intentionally or by omission, after having knowledge of a security breach and of the obligation to notify the National Privacy Commission pursuant to Section 20(f) of the Act;
- Disclosing by any personal information controller or personal information processor or any of its officials, employees or agents, to a third party personal information or sensitive personal information without the consent of the data subject and without malice or bad faith;
- Disclosing, with malice or in bad faith, by any personal information controller or personal information processor or any of its officials, employees or agents of unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her.

ELECTRONIC MARKETING

In 2008, the Department of Trade and Industry, the Department of Health, and the Department of Agriculture issued a joint administrative order implementing the Consumer Act of the Philippines (Republic Act No. 7394) and the E-Commerce Act (Republic Act No. 8792). The Joint DTI-DOH-DA Administrative Order No. 01 (the "Administrative Order") provides rules and regulations protecting consumers during online transactions, particularly on the purchase of products and services. It covers both local and foreign-based retailers and sellers engaged in e-commerce.

The Administrative Order particularly requires retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce with consumers to refrain from engaging in any false, deceptive and misleading advertisement prohibited under the provisions of the Consumer Act of the Philippines.

In line with the Administrative Order's provision on fair marketing and advertising practices, retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce are mandated to provide:

- fair, accurate, clear and easily accessible information describing the products or services offered for sale such as the nature, quality and quantity thereof;
- fair, accurate, clear and easily accessible information sufficient to enable consumers to make an informed decision whether or not to enter into the transaction; and
- such information that allows consumers to maintain an adequate record of the information about the products and services offered for sale.

Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012"[2] (the "CPA") prohibits and penalizes unsolicited commercial communications unless:

- there is prior affirmative consent from the recipient; or

[2] The CPA was signed into law on 12 September 2012. However, the Philippine Supreme Court issued a temporary restraining order dated 9 October 2012 on the law's implementation. The order is effective for 120 days and is set to expire on 6 February 2013. Oral arguments were conducted on 15 January 2013 where a request for an extension of such restraining order was made. As of 20 January 2013, The Supreme Court has yet to act on such extension.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or
- the following conditions are present:
  - The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;
  - The commercial electronic communication does not purposely disguise the source of the electronic message; and
  - The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The CPA is the first law in the Philippines which specifically criminalizes computer crimes. The law aims to address legal issues concerning online interactions. The CPA does not define nor does it particularly refer to online privacy, however, it penalises acts that violate an individual's rights to online privacy, particularly those interferences against the confidentiality, integrity and availability of computer data and systems.

Law enforcement authorities, with due cause, shall be authorised to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system. "Traffic data" as used in the CPA, refers to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seised or disclosed will require a court warrant.

The court warrant shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce showing that there are:

- reasonable grounds to believe that any of the crimes penalised by the CPA has been committed, or is being committed, or is about to be committed;
- reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and
- no other means readily available for obtaining such evidence.

The integrity of traffic data shall be preserved for a minimum period of six months from the date of the transaction.

Courts may issue a warrant for the disclosure of traffic data if such disclosure is necessary and relevant for the purposes of investigation in relation to a valid complaint officially docketed.

No law in this jurisdiction currently deals with the subject of Location Data or the regulation of the use of Cookies.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

44. POLAND

CONTRIBUTION DETAILS

Prof. dr hab. Krystyna Szczepanowska – Kozłowska
Partner
T +48 22 540 74 02
krystyna.szczepanowska@dlapiper.com

Dagmara Jaskulak
Associate
T +48 22 540 74 57
dagmara.jaskulak@dlapiper.com

LAW

As a member of European Union, Poland implemented EU Data Protection Directive 95/46/EC in the Personal Data Protection Act of 29 August 1997 (consolidated text Journal of laws of 2002, No 101, item 926 as amended, hereinafter referred to as the "**PDPA**"). The implementation was introduced by the Amendment of Certain Laws in Connection with Membership of the Republic of Poland in the European Union of 24 August 2007 (Journal of laws of 2007, No 176, item 1238).

DEFINITION OF PERSONAL DATA

The PDPA states that personal data shall mean any information relating to an identified or identifiable natural person. An identifiable person is the one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. A piece of information shall not be regarded as identifying where the identification requires an unreasonable amount of time, cost and manpower.

DEFINITION OF SENSITIVE PERSONAL DATA

Pursuant to the PDPA sensitive personal data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership, as well as personal data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

General Inspector of Personal Data Protection
(*Generalny Inspektor Ochrony Danych Osobowych*)
Stawki 2
00-193 Warsaw, Poland
T (22) 860 70 86 or (22) 860 70 70 (hot-line)
F (22) 860 70 86
kancelaria@giodo.gov.pl

REGISTRATION

As a general rule, data controllers who process personal data must notify the General Inspector about the data filing system containing such data. The General Inspector keeps a register of data controllers and data filing systems, which is available to the public.

The obligation to register data filing systems does not apply to the data controllers of data which:

- include confidential information;
- were collected as a result of inquiry procedures conducted by officers of bodies authorised to conduct such inquiries;
- are processed by relevant bodies for the purpose of court proceedings and on the basis of the provisions on the National Criminal Register;
- are processed by the Inspector General of Financial Information;
- are processed by relevant bodies for the purpose of Poland's participation in the Schengen Information System and Visa Information System;
- are processed by relevant bodies on the grounds of laws which regulate the exchange of information with law enforcement agencies of EU Member States;
- relate to the members of churches or other religious unions with an established legal status, being processed for the purposes of these churches or religious unions;
- are processed in connection with the employment by the controller or providing services for the controller on the grounds of civil law contracts, and also refer to the controller's members and trainees;
- refer to the persons availing themselves of health care services, notarial or legal advice, patent agent, tax consultant or auditor services;
- are created on the basis of electoral regulations concerning the Lower Chamber of the Polish Parliament, the Senate, the European Parliament, communal councils, district councils and provincial councils, the President of the Republic of Poland, the head of a commune, the mayor or president of a city, and acts on national referendums and municipal referendums;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- refer to persons deprived of freedom under the relevant law within the scope required for carrying out the provisional detention or deprivation of freedom;
- are processed for the purpose of issuing an invoice, a bill, or for accounting purposes;
- are publicly available;
- are processed in the preparation of a thesis required to graduate from a university or be awarded a degree; or
- are processed with regard to minor, everyday affairs.

The data controller may start the processing of data in the data filing system after notification of the system to the General Inspector, unless the controller is exempted from this obligation. Nevertheless, the data controller of sensitive data may start the processing of these data in the data filing system after registration of the file, unless the data controller is exempted from the obligation to submit the system for registration.

The notification should include, in particular, the following information:

- the identity of the data controller and any data processors;
- the legal grounds for data processing;
- the purpose of the processing;
- a description of the categories of the data subjects;
- the scope of processing of the data;
- the means of data collection and disclosure;
- a description of the technical and organisational measures undertaken in order to comply with the goals defined in the PDPA; and
- information relating to the possible data transfer to a third country.

DATA PROTECTION OFFICERS

The data controller is obliged to appoint an administrator of information security who supervises the compliance with security measures implemented in order to protect the personal data against their unauthorised disclosure, takeover by an unauthorised person, processing with the violation of the PDPA, any change, loss, damage or destruction.

COLLECTION AND PROCESSING

The processing of data is permitted only if:

- the data subject has given his/her consent, unless the processing consists in erasure of personal data;
- processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for the performance of tasks provided for by law and carried out in the public interest; or
- processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject.

Where sensitive data is processed, one of the following conditions must be met:

- the data subject has given his/her written consent, unless the processing consists of the erasure of personal data;
- the specific provisions of other statutes provide for the processing of such data without the data subject's consent and provide for adequate safeguards;
- processing is necessary to protect the vital interests of the data subject, or of another person, where the data subject is physically or legally incapable of giving his/her consent until he establishes who is the guardian or curator;
- processing is necessary for the purposes of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non profit organisations or institutions with a political, scientific, religious, philosophical, or trade union aim provided that the processing relates solely to the members of those organisations or institutions or to the persons who have a regular contact with them in connection with their activity and subject to providing appropriate safeguards of the processed data;
- processing relates to the data necessary to pursue a legal claim;
- processing is necessary for the purposes of carrying out the obligations of the controller with regard to employment of his/her employees and other persons, and the scope of processing is provided by the law;
- processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards;
- the processing relates to those data which were made publicly available by the data subject;
- it is necessary to conduct scientific research including preparations of a thesis required for graduating from university or receiving a degree; any results of scientific researches shall not be published in a way which allows identifying data subjects; and
- data processing is conducted by a party to exercise the rights and duties resulting from decisions issued in court or administrative proceedings.

The data controller is obliged to provide a data subject with information including: the identity of the data controller, the purpose of data collection, the data recipients or categories of recipients, if known at the date of collecting, the existence of the data subject's right of access

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

to his/her data and the right to rectify these data, whether the replies to the questions are obligatory or voluntary, and in case of existence of the obligation about its legal basis. Further information is required if personal data has not been obtained from a data subject.

TRANSFER

The transfer of personal data to a third country (i.e. a country outside the European Economic Area) may take place only if the country of destination ensures an adequate level of data protection.

The adequate level of protection of personal data is evaluated taking into account all the circumstances surrounding the data transfer, in particular taking into account the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination of the data, the laws applicable in the third country, safety measures used in this country and business conduct.

Nevertheless, the data controller may transfer the personal data to a third country provided that:

- the data subject has given his/her written consent;
- the transfer is necessary for the performance of a contract between the data subject and the controller or takes place in response to the data subject's request;
- the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject;
- the transfer is necessary or required by reasons of public interest or for the establishment of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer relates to data which are publicly available.

In cases other than those referred to above, the transfer of personal data to a third country which does not ensure at least the same level of personal data protection as that in force in Poland may take place only subject to the prior consent of the General Inspector, provided that the data controller ensures adequate safeguards with respect to the protection of the privacy, rights and freedoms of the data subject (the use of "standard contractual clauses" approved by the European Commission, or the implementation of Binding Corporate Rules easing the granting of such approval).

For the transfer of data to United States, compliance with US/EU Safe Harbor principles satisfies the requirement of the PDPA and the consent of the General Inspector is not required.

The transfer of personal data is also allowed if it is required by legal provisions or by the provisions of any ratified international agreement which guarantees an adequate level of personal data protection.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

The data controller is obliged to implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and to protect data against unauthorised disclosure, takeover by an unauthorised person, processing which violates the PDPA, any change, loss, damage or destruction, and in particular the data controller should:

- keep the documentation describing the way of data processing and security measures;
- appoint an administrator of information security who supervises the compliance with security measures;
- grant authorisation to persons who are allowed to carry out the processing of data;
- ensure supervision over the following: which data, when and by whom have been entered into the filing system and to whom they are transferred; and
- keep a register of persons authorised to carry out the processing of data.

There are three levels of security measures depending on the category of data: "basic", "medium" and "high". In the event no sensitive data is processed and none of the devices of the IT system used for data processing is connected with the public network (i.e. the Internet) security measures should be applied at a basic level. If the data controller processes sensitive data, security measures should be applied at least at the medium level. If at least one device of the IT system used for data processing is connected to the public network, security measures should be applied on the high level.

BREACH NOTIFICATION

There is no requirement in the PDPA to report data security breaches or losses to the General Inspector or to data subjects. However, pursuant to the Polish Code on Criminal Procedure there is a civic duty to inform the state prosecutor or Police in case of the commission of an offence prosecuted ex officio. Non compliance with the PDPA is an offence.

ENFORCEMENT

In Poland the General Inspector is responsible for the enforcement of the PDPA.

Where there is a breach of the provisions on personal data protection, the General Inspector *ex officio* or upon a motion of a person concerned, by means of an administrative decision, may issue orders to restore the proper legal state. Failure to comply with the decision is subject to fines up to approximately EUR 50,000.

Furthermore, non compliance with the PDPA may be a criminal offence. A person who is liable (usually a member of a management board of the company which is a data controller) may be subject to a fine (from approximately EUR 25 to approximately EUR 270,000), a partial restriction of freedom or a prison sentence of up to three years.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

Electronic marketing activities are subject to the regulations of the PDPA, the Act of 18 July 2002 on Providing Services by Electronic Means (Journal of Laws of 2002, No 144, item 1204 as amended ("**PSEM**") and the Telecommunications Act of 16 July 2004 (Journal of Laws of 2004, No 171, item 1800 as amended ("**Telecommunications Act**").

The PDPA applies to electronic marketing activities as such activities will involve processing of personal data, eg an e-mail address is likely to be considered personal data for the purposes of the PDPA. The PDPA lays down the grounds for processing of personal data for marketing purposes. According to the PDPA the data controller may process personal data if processing is necessary for the purpose of legitimate interests pursued by the data controllers provided that the processing does not violate the rights and freedoms of the data subject.

The legitimate interests includes direct marketing of own products or services provided by the data controller. Therefore, if marketing activities relate only to products and services owned by the data controller, consent for such processing is not required. The data subject may always object to such processing. Nevertheless, if marketing activities relate to products and services not owned by the data controller, prior consent for such processing is necessary. In each case the data subject should be informed about processing of his/her personal data for marketing purposes.

Apart from consent for processing of personal data (if such consent is required), the PSEM imposes an obligation to obtain a separate consent for sending marketing information by electronic means, (eg e-mails and SMS). The consent should not be presumed to be or be part of another statement of will and may be withdrawn at any time. Sending commercial information without consent is considered to be unfair competition practice. A service provider should be able to provide evidence that it has obtained consent.

The Telecommunications Act prohibits the use of automated calling systems for direct marketing, unless a user has given prior consent to this. The consent of the user:

- may not be presumed or implied by a declaration of will of a different content;
- may be expressed by electronic means, provided that it is recorded and confirmed by the user; and
- may be cancelled at any time, in a simple manner and free of charge.

Enforcement and sanctions – Failing to fulfill the obligations to obtain consent for using automated calling systems for direct marketing is subject to a financial penalty up to 3% of the revenues of the fined company for the past calendar year. The penalty is imposed by the President of the Office of Electronic Communication (hereinafter referred to as the "**President of OEC**"). In addition, the President of OEC may impose a financial penalty on a person in charge of the company up to 300% of his/her monthly remuneration.

Sending marketing information by electronic means without consent is subject to criminal liability (a fine) and is considered to be an act of unfair competition.

The sanctions relating to PDPA set out in the Enforcement section above will apply accordingly.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The Telecommunications Act regulates the collection of transmission and location data and the use of cookies (and similar technologies). The amendment to the Telecommunications Act which implements Directive 2009/136/EC and Directive 2009/140/EC came into force on 21 January 2013, with the exception of the new provisions regarding cookies, which will come into force by 22 March 2013.

Transmission data – The processing of transmission data (understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or as a part of telecommunications services indicating geographic location of terminal equipment of a user of publicly available telecommunications services) for marketing telecommunications services or for providing value-added services is permitted if the user gives his/her consent.

Data about location – In order to use data about location (understood as location data beyond the data necessary for message transmission or billing), a provider of publicly available telecommunications services has to:

- obtain the consent of the user to process data about location concerning this user, which may be withdrawn for a given period or in relation to a given call; or
- perform the anonymisation of this data.

A provider of publicly available telecommunications services is obliged to inform the user, prior to receiving its consent, with regard to the type of data about location which is to be processed, with regard to the purpose and time of its processing, and whether this data is to be passed on to another entity in order to provide a value-added service.

Data about location may be processed only where this is necessary to provide value-added services.

Cookies – The use and storage of cookies and similar technologies requires:

- providing clear and comprehensive information to the user;
- obtaining the consent of the user; and
- that stored information or gaining access to this stored information does not cause configuration changes in the telecommunications device of the user or the software installed on this device.

The user may grant consent by using the settings of the software installed in the final telecommunications device used by him/her or by the service configuration.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

According to the explanations of the Ministry of Administration and Digitalisation, which has prepared the amendment to the Telecommunications Act, consent can be inferred by a user's actions, e.g. the user is given clear and relevant information about the cookies that are used and on that basis gives his/her consent by changing browser settings.

Consent is not required if storage or gaining access to cookies is necessary for:

- transmitting a message using a public telecommunications network; or
- delivering a service rendered electronically, as required by the user.

Enforcement and sanctions – A company that processes transmission data contrary to the Telecommunications Act or fails to fulfill obligations to obtain consent for processing data about location or storing and gaining access to cookies is subject to a financial penalty up to 3% of the company's revenues for the past calendar year. The penalty is imposed by the President of OEC. In addition, the President of OEC may impose a financial penalty on a person in charge of the company up to 300% of his/her monthly remuneration.

The sanctions relating to PDPA set out in the Enforcement section above will apply accordingly.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

45. PORTUGAL

CONTRIBUTION DETAILS

ABBC

Azevedo Neves, Benjamim Mendes, Carvalho & Associates – is a full service law firm established in Portugal since 2007
ABBC has been DLA Piper's focus firm in Portugal since 2011
www.abbc.pt

Joao Costa Quinta

Partner
j.quinta@abbc.pt

Ana Mira Cordeiro

Associate
a.cordeiro@abbc.pt

LAW

Portuguese Data Protection Law – Law nº. 67/98, of October 26th – was enacted pursuant to Directive 95/46/EC.

DEFINITION OF PERSONAL DATA

The Portuguese Data Protection Law defines "personal data" as any given information, in any format, including sound and image, related to a specific or an identifiable natural person ("**data subject**") An identifiable person is one who can be identified, directly or indirectly, namely by reference to a specific number or to one or more elements concerning his/her physical, physiological, mental, economic, cultural or social identity.

DEFINITION OF SENSITIVE PERSONAL DATA

Article 7 of the Data Protection Law defines "sensitive personal data" as any personal data revealing one's philosophical or political beliefs, political affiliations or trade union membership, religion, private life and racial or ethnic origin and also data concerning health or sex life, including genetic data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Comissão Nacional de Protecção de Dados ("National Commission for the Protection of Data" also known as **"CNPD"**).
Rua de São Bento nº. 148, 3º
1200-821 Lisbon
T +351 21 392 84 00
F +351 21 397 68 32
geral@cnpd.pt
www.cnpd.pt

REGISTRATION

Data controllers who process personal data shall notify the Data Protection Authority (CNPD), unless an exemption applies. For certain categories of data (sensitive data when permitted, data regarding illicit activities or criminal and administrative offenses or credit and solvability data) and certain specific processing, prior authorization from CNPD is required. Any variations or changes to the processing of personal data will determine the amendment of the registration.

As for the filing requirements, CNPD has an official form that must be submitted in Portuguese with the following information:

- Identity of the controller and its representative;
- Main software features;
- The purposes of the processing;
- Third party entity responsible for the processing (if applicable);
- All the personal data that will be collected in each register; it is also necessary to indicate if sensitive data is to be collected as well as data concerning the suspicion of illegal activities, criminal and/or administrative offences, as well as data regarding credit and solvability.
- Grounds of legitimacy of the collection and a brief description of the data collection method used;
- Means and methods available for updating the data;
- Means of communication of data to other entities and their identification (if applicable); and
- Any transfers of data to third countries, listing the reasons, grounds and the measures adopted in each transfer.

DATA PROTECTION OFFICERS

There is no legal requirement in Portugal for organisations to appoint a data protection officer.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

Personal data may only be processed if the data subject has given his/her unambiguous consent or if processing is deemed necessary:

- for the execution of an agreement(s) where the data subject is party or in previous diligences for the conclusion of an agreement at the request of the data subject;
- for the compliance with a legal obligation to which the controller is subject;
- to protect the vital interests of the data subject if the latter is physically or legally unable of giving his/her consent;
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;
- for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Moreover, the data controller must provide the data subject with all the relevant processing information, which includes the identity of the data controller, the purposes of processing and the means made available to the data subject to access, amend and delete its data.

TRANSFER

For the data transfers performed within the EU/EEA countries, it is only required to notify the CNPD and data processing may commence immediately thereafter.

Transfers to non EU/EEA countries can only take place if the recipient country ensures an adequate level of protection. In any case it is mandatory to start an authorization procedure with the CNPD and data processing can only commence upon the authorisation issuance.

Exceptionally, transfers performed according to the standard Model Clauses or to Safe Harbor Certificate holders are possible. In such cases, data processing can be done immediately after filling with CNPD.

SECURITY

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

The adequacy of such measures is assessed considering the state of the art, costs of its implementation, nature of the data and the purpose of processing.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

Law 41/2004, of 18 of August on the protection and processing of personal data in e-communications was recently amended by Law no. 46/2012, of 29 August, which transposed Directive 2009/136/EC.

Now, companies that offer electronic communications services accessible to the public shall, without undue delay, notify the CNPD of a personal data breach. When the personal data breach may affect negatively the subscriber's or user's personal data, companies providing electronic communications services accessible to the public should also, without undue delay, notify the breach to the subscriber or user so that they can take the necessary precautions.

For these purposes, a negative effect to the personal data of privacy exists when the breach may result namely in theft or identity fraud, physical harm, significant humiliation or damage to reputation.

Regardless, if a person/entity is effected by the breach of the Data Protection Law, he/she is entitled to file a claim to the CNPD and/or file a civil lawsuit to seek compensation for damages.

ENFORCEMENT

In Portugal, CNPD is responsible for the enforcement of the Data Protection Law.

The failure to comply with the obligations set forth in the Data Protection Law may be deemed as an administrative and/or criminal offence.

Article 43 determines that any person who intentionally:

- fails to notify or seek CNPD's authorization for data processing;
- provides false information in the notification or in the applications for authorization for the processing of personal data;
- misappropriates or uses personal data in a incompatible manner with the purpose of the collection or with the legalisation instrument;
- promotes or carries out an illegal combination of personal data;
- fails to comply with the obligations provided for in the Data Protection Law or in other data protection legislation when the time limit fixed by the CNPD for complying with them has expired; and
- continues to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act after notification by the CNPD not to do so,

shall be subject to a penalty up to one year's imprisonment or a fine of equivalent to 120 days.

The failure to comply with any of the provisions regarding the conditions and safety of data processing and the observance of the data subjects of information and opposition rights and permanent access to the data shall be deemed as an administrative offence punishable with a fine ranging from EUR 500 and EUR 5,000.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The negligent or inadequate compliance with the obligations referred to above is also punishable by a fine which varies according to the legal nature of the infringer – individuals may be punished with a fine ranging from EUR 250 to EUR 2,500 and corporate entities may be punished with a fine ranging from EUR 1,500 to EUR 15,000.

ELECTRONIC MARKETING

The Law no. 41/2004, of 18 of August on the protection and processing of personal data in e communications was recently amended by Law no. 46/2012, of 29 August, which transposed the 2009/136/EC Directive.

In relation to individuals, the sending of unrequested communications for direct marketing purposes is subject to express prior consent of the subscriber or user (that is, the "opt in" rule applies). This includes the use of automated calling and communication that do not rely on human intervention (automatic call devices), facsimile or electronic mail, including SMS, EMS, MMS and other similar applications.

This does not apply to legal entities and accordingly unrequested direct marketing communications are allowed. Nevertheless, the "opt out" rule applies and legal entities may refuse future communications and enroll in the non-subscribers list.

This does not prevent the supplier of a product or service that has obtained its customers' data and contacts, under the lawful terms of the Data Protection Law and in connection with the sale of a product or service, to use such data for direct marketing of its own products or services similar to those transacted, provided it ensures the customers concerned, clearly and explicitly, with the opportunity to object to the use of such data, free of charge and in an easy manner (i) at the time of the respective collection, and (ii) on the occasion of each message in case the customer has not initially refused such use.

The sending of electronic mail for purposes of direct marketing disguising or concealing the identity of the entity on whose behalf such communication is made, as well as the non-indication of valid means of contact to which the recipient may send a request to stop these communications or the encouragement of recipients to visit websites that violate these provisions, is strictly forbidden. The violation of these rules consists on an administrative offense, punishable with fines ranging from Eur 5,000 to Eur 5,000,000, to legal entities:

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookie compliance – The amended Law no. 41/2004, of 18 of August now determines that the storing of information and the possibility to access information stored in a subscriber/user's terminal is only allowed; (i) on the condition the subscriber/user has provided his or her previous consent; (ii) which must be based on clear and comprehensive information, namely about the purposes of the processing.

This does not prevent technical storage or access; (i) for the sole purpose of carrying out the transmission of a communication over an e-communication network; or (ii) if strictly necessary in order for the provider of an information society service to provide a service expressly requested by the subscriber/user.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

At this point, the local regulatory Authority (CNPD) has not yet issued any guidelines regarding the definition of "consent", namely if implied consent suffices and if the continuous use of website consists consent. In view of Portuguese practice and restrictive approach taken by the DPA, we are of the opinion that implied consent shall not be enough and continuous use of a website shall only be regarded as consent provided clear and evident information is given. The use of a confirmation procedure is advisable.

Traffic Data – Traffic data must be eliminated or made anonymous when no longer needed for the transmission of the communication. Prior express consent is required and may be removed at any time, and only to the extent required and the time necessary to marketing electronic communications services or the provision of value added services.

Processing of traffic data is admissible when required for billing and payment of interconnections and only until the end of the period during which the bill may lawfully be challenged or payment pursued.

Complete and accurate information on the type of data being processed must be provided, as well as the purposes and duration of the processing and the possibility to disclosure to third parties for the provision of value added services. Processing should be limited to workers and employees in charge of billing or traffic management, customer inquiries, fraud detection, marketing of electronic communications services accessible to the public, or the provision of value added services, restricting necessary for the purposes of such activities.

Location Data – Processing of these data is allowed only if they are made anonymous or to the extent and for the duration necessary for the provision of value added services, provided it is obtained prior express consent. Prior information must also be provided.

Companies must ensure the possibility, using simple means and free of charge: (i) to withdraw consent at any time; or (ii) temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.

Non-compliance with "Opt in" rule consists of an administrative offense, punishable with fines ranging from EUR 5,000 to 5,000,000.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

46. ROMANIA

CONTRIBUTION DETAILS

Marian Dinu
Country Managing Partner
T +40 372 155 881
marian.dinu@dlapiper.com

Cosmina Simion
Head of IP, Media & Technology
T +40 372 155 816
cosmina.simion@dlapiper.com

Laura Leanca
Associate
T +40 372 155 814
laura.leanca@dlapiper.com

LAW

Even though Romania has only been a member of the European Union since 1 January 2007, the EU Data Protection Directive 95/46/EC was implemented into national legislation in November 2001 through Law no 677/2001 on the protection of individuals with regards to the processing of personal data and the free movement of such data ("**Data Protection Law**").

DEFINITION OF PERSONAL DATA

"Personal Data" is defined under the Data Protection Law as any information referring to an identified or identifiable natural person. An identifiable person is one who can be identified either directly or indirectly by referring to a personal identification number or to one or several distinctive factors that are typical for the physical, physiological, mental, economic, cultural or social identity of the respective person.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

Under the Data Protection Law, the following categories of data are deemed as sensitive personal data (data presenting special risks): (i) data regarding racial or ethnical origin; (ii) political, religious, philosophical or other similar beliefs; (iii) affiliation to certain unions; (iv) physical or mental health condition; (v) sexual life; (vi) criminal or administrative offences.

Moreover, according to the template notification form issued by the National Supervisory Authority for Personal Data Processing, genetic, biometric data, national identification number, series and number of identification documents are also qualified as sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

National Authority for the Surveillance of Personal Data Processing (in Romanian "***Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal***" or **"ANSPDCP"**).
28-30 Magheru Blvd
District 1, Bucharest
T +40 318 059 211
F +40 318 059 602
www.dataprotection.ro

REGISTRATION

ANSPDCP operates the national registry of data controllers which can be accessible online free of charge. All public and private entities processing personal data must notify ANSPDCP in respect of their personal data processing with at least 30 days in advance and obtain a data controller number, unless an exemption applies.

Based on the standard notification form issued by ANSPDCP, the notification should include the following information:

- the personal data that are being processed (both sensitive and non-sensitive);
- the purpose of processing;
- the categories of targeted data subjects;
- the categories of recipients;
- information regarding the transfer outside Romania, either within the European Economic Area, to states whose level of protection has been considered as adequate by the European Commission or to other third party countries;
- identification details of entities acting as processors on behalf of the data controller;
- the manner in which data subjects are informed regarding their rights: verbally, via a website, or through a document (in which case it must be enclosed);
- the estimated duration of personal data processing; and

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- data security measures. In this sense, the notification must include the security policy of the data controller describing the measures undertakes in order to ensure the security of the personal data processed.

Should the controller process personal data for various purposes, a notification must be filed separately for each purpose, unless such purposes can be correlated.

The notification procedure involves two stages. The first step is to file the online application. The second step is to send by post to ANSPDCP the first page of the notification stamped and signed by the legal representative of the data controller.

Once registered in the general registry, each data controllers shall be allocated a registration number which must be indicated in all official documents of the respective entity relating to the declared purpose of processing.

DATA PROTECTION OFFICERS

Currently, there is no requirement in Romania for data controllers to appoint a data protection officer.

COLLECTION AND PROCESSING

Under Data Protection Law, data controllers may collect and process personal data provided that the data subject has expressly and unequivocally consented thereto. The data subject's consent is not required under the following circumstances:

- the processing is necessary for the performance of a contractual or pre-contractual arrangement where the data subject is a party;
- where the data controller needs to protect the life, physical integrity or health of the data subject or another person;
- the data controller must comply with a legal obligation;
- the processing is necessary for the performance of public interest measures;
- the data controller has a legitimate reason for processing, provided that fundamental civil liberties of data subjects are not breached; or
- processing is performed exclusively for statistical, historical or scientific research purposes.

Where sensitive data is processed, apart from the above conditions, data controllers must comply with additional requirements, depending on the specific type of sensitive data in question.

Data controllers must ensure that the data processed are proportional in relation to the declared purpose of processing, and not excessive.

Data subjects must be thoroughly informed in respect of data processing activities. They must be provided with the following information:

- identity of the data controller and its representative;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- purpose of data processing;
- recipients of personal data and transfer abroad;
- rights provided by law in favour of data subjects as well as their manner of exercise; or
- the consequences of the refusal to provide personal data.

TRANSFER

Different rules shall have to be observed depending on the destination country of such personal data. While personal data transfers outside within the EEA (or to countries with an adequate level of protection) must only be notified to AMSPDCP, transfer to third party countries outside the EEA requires an authorization from ANSPDCP.

If the personal data is transferred to another EU Member State, no other requirement must be met other than ticking the appropriate box in the on line notification form.

In case the data is transferred to a country with an adequate level of data protection (i.e. USA, Argentina, Canada, Switzerland, Jersey, Guernsey, Isle of Man), such countries shall have to be explicitly listed in the on line notification form.

In case the data is transferred to a third party country which is not included in either of the above categories, the transfer is permitted provided that the controller has obtained data subject's consent, or in case it has concluded a data transfer agreement with the recipient of data located in the respective third country. This contract must be submitted with ANPDCP for its review.

For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the Data Protection Law.

ANSPDCP does not recognize intra-group international data transfers based on Binding Corporate Rules.

SECURITY

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

The measures taken must ensure a level of security appropriate to the nature of the data.

Minimum security measures that data controllers must comply with are described in Order no 52/2002 issued by the Romanian Ombudsman.

Data controllers must ensure that when processing data through data processors, the latter have also agreed to comply with data security obligations.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

There is not yet a mandatory requirement in the Data Protection Law to report data security breaches or losses to ANSPDCP or to data subjects.

ENFORCEMENT

ANSPDCD is entitled to investigate any breach of Data Protection Law ex officio or following a complaint filed by a prejudiced data subject. In this sense, ANSPDCP may perform an audit over data processing activities performed by data controllers.

ANSPDCP may impose administrative fines for failure to comply with the Data Protection Law, ranging from approximately EUR 115 to EUR 11,400 (the highest sanction is applied for failure to comply with security measures). The level of fines is higher in case of failure to comply with the regulations in the electronic communications sector, as further detailed below.

Under certain conditions, failure to comply with Data Protection Law may be considered as a criminal offence, in which case ANSPDCP shall contact the competent criminal authorities.

In addition to this, ANSPDCP may impose the temporary suspension of data processing activities as well as the partial or complete deletion of processed data.

According to Data Protection Law, data subjects must be granted the right to oppose to the processing of their personal data for direct marketing purposes (opt-out). The processing of personal data for electronic marketing purposes is further regulated under Law no. 506/2004 on the processing of personal data in the electronic communications sector implementing Directive 2002/58/CE ("**Law 506/2004**"). According to this law, it is forbidden to send commercial communications by using automatic systems that do not require the intervention of a human operator, by fax or electronic mail or any other similar method, except where data subjects have expressly consented in advance. It may be considered that SMS marketing falls under the same restrictions.

Moreover, cases where the data controller has directly obtained the e-mail address of a data subject upon the sale or provision of a certain service towards the latter, the controller may use the respective address for the purpose of sending electronic communications regarding similar products or services, provided that data subjects are clearly and expressly offered the possibility to oppose by way of an easily accessible and free of charge method, not only when the e-mail address is collected but also with each commercial communication received by the data subject.

ANSPDCP has not issued any specific guidelines in relation to electronic marketing.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The processing of traffic data, location data and the implementation of cookies are dealt with under Law 506/2004.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Traffic data – Traffic Data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.

However, traffic data may be retained for the purpose of marketing the services offered to data subjects, or in view of the provision of value added services, solely throughout the marketing period and provided that data subjects have consented to the processing of traffic data.

The processing of traffic data for billing purposes or the establishment of payment obligations for interconnection is permitted solely for a period of three years following the due date of the respective payment obligation.

Data subjects may withdraw their consent at any time.

The provider of electronic communication services must inform data subjects in respect of the processed traffic data, and the duration of processing, prior to obtaining their consent.

Communication service providers and entities acting under their authority may process traffic data for:

- management of billing and traffic;
- dealing with enquiries of data subjects;
- prevention of fraud; or
- the provision of communication services or value added services.

Location data – The processing of such data is permitted in one of the following instances:

- data is rendered anonymous;
- data subjects have consented to such processing for the duration necessary for the performance of value added services; or
- when the purpose of the value added service is the unidirectional and non-differentiated transmission of information towards users.

The service provider must inform the users or subscribers, prior to obtaining their consent, in respect of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent at any time.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, communication service providers must grant users the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Cookies – The storing of cookies on user terminals is permitted subject to the following cumulative conditions:

- users have expressly consented thereto; (Law 506/2004 also provides that consent may be given by way of browser settings or other similar technologies); and
- the information requirements provided by Data Protection Law have been complied with in a clear and user-friendly manner, to include references regarding the purpose of processing of the information stored by users.

Should the service provider allow the storing of third party cookies within a users' computer terminal, they will have to be informed about the purpose of such processing and the manner in which browser settings may be adjusted in order to refuse third party cookies.

Consent is not required where cookies are:

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

Failure to comply with the requirements of Law 506/2004 is classified as a minor offence and is sanctioned with fines ranging from EUR 1,140 to EUR 22,700. In case of companies whose turnover exceeds approximately EUR 1,140,000, the amount of fines may reach up to 2% of the respective company's turnover.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

47. RUSSIA

CONTRIBUTION DETAILS

Michael Malloy
Partner
T +7 495 221 4400
michael.malloy@dlapiper.com

Pavel Arievich
Legal Director
T +7 495 221 4472
pavel.arievich@dlapiper.com

Ekaterina Golodinkina
Associate
T +7 495 221 4546
ekaterina.golodinkina@dlapiper.com

Maria Biryukova
Associate
T +7 495 221 4438
maria.biryukova@dlapiper.com

LAW

Fundamental provisions of data protection law can be found in the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Convention**") ratified by Russia in 2006 and the Russian Constitution establishing the right to privacy of each individual (articles. 23 and 24). There is also specific legislation, including the Data Protection Act No. 152 FZ dated 27 July 2006 ("**DPA**") and various regulatory Acts adopted to implement the DPA as well as the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions which implement the provisions of DPA in relation to specific areas of state services or industries.

DEFINITION OF PERSONAL DATA

Personal data is any information that relates directly or indirectly to the specific or defined physical person (the data subject).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data is defined as special categories of personal data in Russian legislation. Such special categories include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies and biometrical data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Service for Supervision of Communications, Information Technologies and Mass Media or, in short, Roscomnadzor ("**Agency**").
Build. 2, 7, Kitaigorodskiy proezd
Moscow, 109074
T +7 495 987 6800
F +7 495 987 6801
http://www.rsoc.ru/

REGISTRATION

The Agency is in charge of maintaining the Registry of data controllers.

Any data controller shall notify the Agency in writing about its intention to process personal data, unless one of the following exclusions applies:

- The personal data is data about employees;
- The personal data was received in connection with a contract entered into with the data subject, provided that such data is not transferred without the consent of the data subject, but used only for the performance of the contract and entering into contracts with the data subject;
- The personal data is the data about members of a public or religious association and processed by such an organisation for lawful purposes in accordance with their charter documents, provided that such data is not transferred without the consent of the data subjects;
- The personal data was made publicly accessible data by the data subject;
- The personal data includes the surname, name and father's name only;
- The personal data is necessary in order to give single access to the premises of the data controller or for other similar purposes;
- The personal data is included in state automated information systems or state information systems created for the protection of state security and public order;
- The personal data is processed in accordance with the law without any use of automatic devices; or
- The personal data is processed in accordance with transportation security legislation in purposes of procurement of stable and secure transport complex and personal, community and state interests protection.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The notification letter shall contain information about:

- The full name and address of the data controller;
- The purpose of the processing;
- The categories of personal data processed;
- The categories of the subjects whose personal data is processed;
- The legal grounds for processing;
- The types of processing of the personal data;
- The measures of protection of personal data;
- Name and contacts of physical person or legal entity responsible for personal data processing;
- The commencement date;
- Information on occurrence of cross border transfer of personal data;
- The term of processing or the conditions for termination of processing the personal data; and
- Information on personal data security provision.

DATA PROTECTION OFFICERS

If the data controller is a legal entity it shall appoint a data protection officer. Such an appointment is considered to be a personal data protection measure. The data protection officer controls the data controller and its employees regarding the data protection issues, informs them off statutory requirements and organises receiving and processing of communications from data subjects.

COLLECTION AND PROCESSING

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

- The data subject consents;
- The processing is required by a federal law or under an international treaty;
- The processing is required for administration of justice, execution of the court order or any other statements of public officers to be executed;
- The processing is required for provision of state or municipal service;
- The data controller needs to process the data to perform or conclude a contract to which the data subject is a party or beneficiary party or guarantor;
- The processing is carried out for statistical or scientific purposes (except it is also for advertising purposes) provided that it is impersonalised;
- The processing protects the data controller's vital interests and it is impossible to have the data subject's consent;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- The processing is required for execution of statutory controller's or third parties' rights or for purposes important for community provided data subject's rights are not in breach;
- Personal data that is processed was publicly made accessible by the data subject or upon his or her request;
- The processing is carried out by a journalist or mass media as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would damage the data subject's rights and freedoms; or
- Personal data that is processed is subject to publication or mandatory disclosure under law.

As a general rule, consent may be given in any form, but it is the data controller's obligation to provide proof that he has the data subject's consent.

In the following cases the DPA requires that the data subject's consent should be in writing:

- Where the personal data is collected to be included within publicly accessible sources;
- Where sensitive or biometrical data is processed;
- In the case of the cross border transfer of personal data, where the recipient state does not provide adequate protection of personal data; or
- Where a legally binding decision is made solely on the grounds of the automated processing of personal data.

Consent is deemed to have been given in writing where it is signed by hand or given in an electronic form and signed by an electronic signature.

Consent may be revoked.

Consent in writing must contain the following information:

- The identity of the data subject, his/her address and passport details and identity of the subject
- Data representative (if any);
- The identity and address of the data controller or the entity that processes personal data on behalf of the data controller (if any);
- The purpose of the processing;
- The list of personal data that may be collected and processed;
- The types of processing that are authorised;
- The term for which the consent, remains valid and way of revocation; and
- The data subject's signature.

The data controller shall ensure the confidentiality of personal data. The data controller and other persons who have access to the personal data, shall not disclose any information to a third party without a prior consent of the data subject.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

Prior to a transfer of personal data out of Russia, the data controller must ensure that the recipient state provides adequate protection of personal data. The fact that the recipient state ratified the Convention is sufficient grounds to deem that the state provides adequate protection of personal data for the purposes of the DPA.

Where there is no adequate protection of personal data, a cross border transfer is permitted if one of the following conditions is met:

- The data subject consents;
- The transfer is provided for under an international treaty to which Russia is a signatory;
- The transfer is necessary in accordance with federal laws for protection of the Constitution, state defence, security and transport system;
- For the purposes of performance of a contract to which the data subject is party; and
- The transfer protects the data subject's vital interests where it is not possible to get the written consent of the data subject.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, changing, blocking or destruction of, or damage to, personal data.

There is a recent special regulation as to the measures that the data controller should undertake to ensure security of personal data, data systems, carriers of biometrical information and technologies.

BREACH NOTIFICATION

There is no mandatory requirement to report data security breaches or losses to the Agency or to data subjects.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of the DPA.

The Agency is entitled to:

- Carry out checks;
- Consider complaints from data subjects;
- Require the submission of necessary information about personal data processing by the data controller;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Require the undertaking of certain actions according to the law by the data processor, including discontinuance of the processing of personal data;
- File court actions;
- Initiate criminal cases; and
- Impose administrative liability.

If the Agency becomes aware that a data controller is in violation of the law, he can serve an enforcement notice requiring the data controller to rectify the position.

A data controller can face civil, administrative or criminal liability if there is a violation of personal data law. Officers of the data controller responsible for the offence may face disciplinary action.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the position to be rectified and may also impose an administrative penalty and/or recommend imposing disciplinary action on the officers of the data controller who are responsible for the offence.

The maximum administrative penalty that can be imposed, as at the date of this review, is EUR 10,000. Lately, there has been much discussion at about dramatically increasing the administrative penalty.

ELECTRONIC MARKETING

Electronic marketing activities are subject to limitations set by the Russian Law on Advertising No. 38-FZ dated 13 March 2006 ("**AA**"), under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only subject to preliminary consent of a subscriber or addressee to receive advertising.

Advertising is presumed to be distributed without preliminary consent of the subscriber or addressee unless the advertising distributor can prove that such consent was obtained. The advertising distributor is obliged immediately to stop distribution of advertising to the address of the person who made such a demand.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Russian law does not specifically regulate online privacy. The definition of personal data under the DPA is rather broad and there are views that information on number, length of visits of particular web-sites and IP address (in combination with other data allowing the user to be identified) could be considered personal data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

48. SINGAPORE

CONTRIBUTION DETAILS

Amica Law LLC
30 Raffles Place
#18-03/04 Chevron House
Singapore 048622

Geraldine Tan
Associate Director
T +65-6303 6221
geraldine.tan@amicalaw.com

LAW

Singapore recently enacted a new Personal Data Protection Act 2012 (No. 26 of 2012) ("**Act**") on 15 October 2012. The Act will take effect in 3 phases:

- Provisions relating to the formation of the Personal Data Protection Commission ("**Commission**") came into force on 2 January 2013;
- Provisions relating to the National Do-Not-Call Registry ("**DNC Registry**") will come into force in early 2014; and
- The main data protection provisions will come into force in mid-2014.

The phased implementation of the Act serves as a transition period for organisations to review and adopt internal personal data protection policies and practices, so that they may comply with the Act. The exact dates on which the DNC Registry provisions and other data protection provisions will come into force will be announced at a later date.

DEFINITION OF PERSONAL DATA

"Personal data" is defined in the Act to mean data, whether true or not, about an individual who can be identified;

- from that data; or
- from that data and other information to which the organisation has or is likely to have access.

DEFINITION OF SENSITIVE PERSONAL DATA

There is no definition of "sensitive personal data" in the Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Personal Data Protection Commission
T +65 6377 3131
F +65 6273 7370
info@pdpc.gov.sg
http://www.pdpc.gov.sg/

REGISTRATION

There are no registration requirements under the Act.

DATA PROTECTION OFFICERS

Each organisation is required to appoint one or more data protection officers to be responsible for ensuring the organisation's compliance with the Act. The contact details of at least one of these data protection officers must be published.

COLLECTION AND PROCESSING

Organisations may only collect, use, or disclose personal data where:

- they obtain consent from the individual prior to the collection, use, or disclosure of the personal data;
- there is deemed consent by the individual to the collection, use, or disclosure of the personal data; or
- if no consent or deemed consent is given, in specific circumstances prescribed in the Act.

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the organisation.

Further, any collection, use or disclosure of the personal data must only be for the purposes that a reasonable person would consider appropriate in the circumstances, and for purposes to which the individual has been notified of. Such notification must be made in accordance with the requirements of the Act.

TRANSFER

Transfer of personal data out of Singapore is allowed, provided that the organisation ensures that a comparable standard of protection (as set out in the Act) is accorded to personal data that is to be transferred overseas.

An organisation may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Minister for Communications and Information may require.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Organisations are obligated to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The Act does not specify specific security measures to adopt and implement.

BREACH NOTIFICATION

Currently, there are no specific legislative requirements for data users to notify authorities regarding data protection breaches in Singapore.

Aggrieved parties may either make a complaint to the Commission, or may take out a private action in civil proceedings. The Commission may also conduct investigations on its own motion.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission. The powers of the Commission include giving directions to:

- stop collection, use or disclosure of personal data in contravention of the Act;
- destroy personal data collected in contravention of the Act;
- provide or refuse access to or correction of personal data; and/or
- pay a financial penalty not exceeding $1 million.

These directions may be registered with the Singapore District Courts so that they may have the force and effect of an order of court.

Directions or decisions given are subject to reconsideration by the Commission, upon written application by any aggrieved party.

Directions, decisions or reconsiderations of the Commission may also be subject to appeal to a Data Protection Appeal Committee, unless the direction or decision to be appealed is the subject of an application for reconsideration, in which case such appeal would be deemed withdrawn.

Directions may only be appealed to the High Court and Court of Appeal with regard to:

- a point of law arising from a direction or decision of the Appeal Committee; or
- any direction of the Appeal Committee as to the amount of a financial penalty.

Any person who has suffered loss or damage directly as a result of a contravention the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only lie after the decision has become final as a result of there being no further right of appeal. The court may grant to the plaintiff all or any of the following:

- Relief by way of injunction or declaration;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Damages; and/or
- Such other relief as the court thinks fit.

ELECTRONIC MARKETING

The Act will apply to electronic marketing activities, to the extent that there is any collection, use or disclosure of personal data by an organisation.

Further, the Act provides that no person or organisation is to conduct electronic marketing activities by sending a specified message to a Singapore telephone number, unless such person or organisation has checked and received confirmation from the Commission that the telephone number is not on a Do-Not-Call register maintained by the Commission ("**DNC Register**"). An individual may apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

Specified messages include messages that are sent with one of the following purposes:

- To offer to supply goods or services;
- To advertise or promote goods or services;
- To advertise or promote a supplier, or prospective supplier, of goods or services;
- To offer to supply land or an interest in land;
- To advertise or promote land or an interest in land;
- To advertise or promote a supplier, or prospective supplier, of land or an interest in land;
- To offer to provide a business opportunity or an investment opportunity;
- To advertise or promote a business opportunity or an investment opportunity;
- To advertise or promote a provider, or prospective provider, of a business opportunity or an investment opportunity; or
- Any other prescribed purpose related to obtaining or providing information.

"Message" is defined in the Act to mean any message, whether in sound, text, visual or other form. This includes any voice calls, faxes, Short Messaging Service (SMS) or Multimedia Messaging Service (MMS).

The Act will apply to specified messages addressed to a Singapore telephone number where:

- the sender of the specified message is present in Singapore when the specified message was sent; or
- the recipient of the specified message is present in Singapore when the message is accessed.

Electronic marketing activities are also regulated under the Spam Control Act (Cap 311A), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

49. SLOVAK REPUBLIC

CONTRIBUTION DETAILS

JUDr. Dr. Michaela Stessl
Country Managing Partner
T +421 2 59202 122
M +421 902 955 984
michaela.stessl@dlapiper.com

LAW

As a member of the European Union, Slovakia implemented the EU Data Protection Directive 95/46/EC in September 2002 with Act No. 428/2002 Coll., the Data Protection Act, as amended ("**DPA**").

DEFINITION OF PERSONAL DATA

Personal data shall, for the purposes of the DPA, mean any information relating to an identified or identifiable natural person, either directly or indirectly, in particular by reference to an identifier of general application or by reference to one or more factors specific to his/her physical, physiological, psychic, mental, economic, cultural or social identity.

DEFINITION OF SENSITIVE PERSONAL DATA

The DPA does not provide for a definition of sensitive personal data. However, one of the provisions of the DPA namely "Special categories of data" refers, *inter alia*, to personal data related to race, ethnic origin, political opinions, religious belief, as well as data related to the breach of provisions of criminal or civil law, biometrical data, or data related to the mental status of the data subject.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Office of the Slovak Republic ("**Office**") is: Úrad na ochranu osobných údajov Slovenskej republiky (Official Slovak Name)
Hraničná 12
820 07, Bratislava 27
Slovak Republic

The Office is responsible for overseeing the DPA in Slovakia.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

Data controllers need to register information systems with the Office under the conditions set out in the DPA.

The obligation to register applies to all information systems in which personal data is processed fully or partially by an automated means of processing unless a statutory exception applies. The information system needs to be registered before starting with the processing of the data contained therein. The Office will carry out the registration free of charge and it will assign a registration number to the pertinent information system, as well as issue a certificate confirming its registration. If it is unclear whether the particular information system is subject to registration, the Office will issue a binding decision.

Special registration applies to information systems defined in the DPA, *inter alia*, those that contain special categories of data or data processed without the data subject's consent, which is to be transferred to third countries that do not guarantee an adequate level of data protection. The Office will assess the submitted data, verify whether the data processing could infringe the rights and freedoms of data subjects and decide, within 60 days from the day of its receipt, whether or not it will permit the data processing. If the Office assesses the data processing in the information system as a risk, it shall prohibit the processing for the respective purpose.

DATA PROTECTION OFFICERS

The data controller is responsible for the internal supervision of protection of personal data processed pursuant to the DPA. The data controller is required to nominate in writing one or more data protection officers for supervising the observation of the DPA provisions in his/her/its company if he/she/it employs more than five people. The Office must be notified of this fact in writing by the data controller without undue delay, but no later than 30 days from such nomination.

COLLECTION AND PROCESSING

Under the DPA, the data controller who intends to collect personal data from the data subject must inform the data subject, no later than obtaining the data, and notify him/her in advance of the following:

- The business name and registered office or permanent residence of the data controller;
- The business name and registered office or permanent residence of the data processor, provided that the data processor obtains personal data on behalf of the data controller or the data controller's representative;
- The purpose of the personal data processing; and
- Additional information in the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data, the particulars of which are provided in the DPA.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Personal data may be processed only by the data controller or data processor. The data processor may process personal data only to the extent and under the conditions agreed with the data controller in a written contract or by written authorisation.

The DPA lists basic obligations of the data controller mentioned below. The data controller must, *inter alia*:

- determine unambiguously and specifically the purpose of data processing before starting the data processing; the purpose of data processing must be clear and it cannot be contrary to the Constitution of the Slovak Republic, constitutional laws, laws and international treaties binding for the Slovak Republic;
- determine the means and manner of the data processing and, if appropriate, other conditions of the data processing;
- process only accurate, complete and, where necessary, updated personal data in respect of the purpose of its processing;
- destroy the personal data when the purpose of processing is terminated; and
- process personal data in accordance with public morals and act in a manner not contrary to, or circumventing, the DPA or other generally binding legal regulations.

Personal data may only be processed upon the consent of the data subject, unless provided otherwise for by the DPA. Under the DPA, the processing of special categories of data (i.e. sensitive information) is allowed only upon the written consent of the data subject and following the specific conditions set forth in the DPA.

TRANSFER

Transfer to third parties within the territory of the Slovak Republic. The personal data of the data subject may be transferred from the information system to another natural person or legal entity only upon the written confirmation on the data subject's consent obtained, if the DPA requires such consent; the person providing data in such manner may replace this written confirmation by a written declaration of the data controller stating that the data subjects gave their consent, provided that the data controller is able to prove that the written consent of the data subjects was given.

Transfer to non-EU member states that offer an adequate level of data protection. If the third country guarantees an adequate level of data protection, the data may be transferred to this country if the data controller informed the data subject about the facts required to obtain the data subject's data (i.e. the information mentioned above in relation to data collecting by the data controller). Under the DPA, the data transfer to a country that guarantees an adequate level of protection is also allowed in cases when a notification/information to the data subject is not required.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Transfer to third countries (excluding the US) that do not offer an adequate level of data protection. If the third country does not guarantee an adequate level of protection, the transfer of data is possible only on the basis of a decision of the European Commission or if any of the conditions mentioned below is fulfilled:

- The data subject gave a written consent to the transfer, while knowing that the country of final destination does not ensure an adequate level of protection;
- The transfer is necessary for the execution of a contract between the data subject and the data controller or for pre contractual measures, upon the request of the data subject;
- It is necessary for entering into, or the execution of, a contract concluded by the data controller in the interest of the data subject with another entity,
- It is necessary for the execution of an international treaty binding for the Slovak Republic or resulting from the laws due to an important public interest or for proving, filing or defending a legal claim;
- It is necessary for the protection of vital interests of the data subject; or
- It concerns the personal data, which constitutes a part of the lists, registers or files and are kept and publicly accessible pursuant to special legislation or is available, under this legislation, to persons who prove that they are legally entitled and fulfil the conditions prescribed by law for making the data available.

If the data controller decides to transfer personal data to a third country, which does not guarantee an adequate level of protection, after obtaining the personal data, it must inform the data subject before the transfer of the personal data about the reason of its decision and advise the data subject about his/her right to refuse consent with such transfer, if this consent is required; the data controller shall be entitled to execute the proposed transfer of the personal data only after obtaining the written consent of the data subject.

If the data controller authorises an entity residing abroad for the data processing on the data controller's behalf, this entity shall be entitled to process the personal data only to the extent and under the conditions agreed with the data controller in a written contract. The scope of the contract must be elaborated in accordance with the standard contractual terms set by Decision of the European Commission L39/5 from February 5, 2010, notified under Document C (2010) 593 stipulated for the transfer of personal data by an entity residing abroad processing data on the data controller's behalf. The consent of the Office is required for this transfer of personal data.

Transfer to the US. For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the DPA provisions on data transfer. The Office will ascertain whether or not the US company, which will be the data importer, did sign up for the Safe Harbor principles. This US company must file an application for approval of the data transfer to the US with the Office. Provided that this company is a member of the Safe Harbor principles and the application is correct and complete, the Office will grant its approval.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

The data controller and the data processor are responsible for the security of personal data by protecting it against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorised access and making available, as well as against any other unauthorised forms of processing. For this purpose, the data controller must take reasonable technical, organisational and personal measures which correspond to the manner of processing data.

The data controller is required to prepare a so called security project of the information system where the information system contains certain special categories of data. The data controller is required to nominate in writing one or more data protection officers for supervising the observation of the DPA provisions in his company if he employs more than five people. The data controller is required to instruct the entitled persons about the rights and obligations stipulated in the DPA and about the liability for their violation. The data controller must establish and maintain confidentiality of the processed data even after the conclusion of its processing.

BREACH NOTIFICATION

Under the DPA, there is no mandatory requirement to report data security breaches or losses to the Office. However, this does not affect the possibility of other public authorities to report data security infringements or losses to the Office if they suspect that such an event might have occurred.

ENFORCEMENT

The Office is responsible for the enforcement of the DPA. Upon a complaint from a data subject or another person or a report from public authorities, the Office shall commence administrative proceedings to ascertain possible breaches of obligations or conditions stipulated by the DPA and eventually can impose a fine for these breaches. The Office may issue decisions to provide temporary relief for the data subject or to ensure due rectification depending on the nature of the breach.

The Office may impose fines for breaches of the DPA between EUR 330 to EUR 332.000. The Head of the Office or the Chief Inspector may publish a notice containing the identity of the data controller or data processor that breached or circumvented the provisions of the DPA and the final decision of the Office regarding such breach, including its descriptions, and merits of the case. The Office may also impose disciplinary fines on the data controller or the data processor in instances stipulated by the DPA.

ELECTRONIC MARKETING

Electronic marketing shall be governed by Act No. 351/2011 Coll. on Electronic Communications, as amended ("**ECA**").

Under the ECA, processing of the traffic data of a subscriber or user for the purposes of marketing services or purposes of ensuring the value added services by any public network or service providers is possible solely with the prior consent of the subscriber or the user.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Prior to obtaining the consent, the public network or service providers are obliged to inform the subscriber or user on (i) the type of the traffic data processed, (ii) the purpose of the traffic data processing and (iii) the duration of the data processing.

For the purposes of direct marketing, the call or use of automatic calls and communications systems without human intervention, facsimile machines, e-mail, including SMS messages to the subscriber or user, who is a natural person, is allowed solely with his/her prior consent. Such consent shall be proved. Users or subscribers are entitled to withdraw such consent at any time.

The prior consent of the recipient of a marketing e-mail shall not be required in the case of direct marketing of own similar products and services of a person, that has obtained electronic contact information of the recipient from the previous sale of its own product and/or service to such recipient and in line with the provisions of the ECA. The recipient of an e-mail shall be entitled to refuse at any time, by simple means and free of charge such use of electronic contact information at the time of its collection and on the occasion of each message delivered in the case the recipient has not already refused such use.

Both, (i) sending e-mails for the purposes of direct marketing without the determination of a valid address to which the recipient may send a request that he/she is no longer willing to receive such communication and (ii) encouragement to visit a website in contradiction with a special regulation, shall be prohibited.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

As regards the protection of privacy and protection of personal data processed in the electronic communications sector, the provisions of the ECA shall apply. The ECA implemented Directive 2002/58/EC (as amended by Directive 2009/136/EC).

Under the ECA, the public network or service providers is obliged to ensure technically and organisationally the confidentiality of the communications and related traffic data, which are conveyed by means of its public network and public services. In particular recording, listening, storage of data (or other kinds of an interception or a surveillance of communications and data related thereto) by persons other than users, or without the consent of the concerned users, shall be prohibited. However, this does not prohibit the technical storage of data, which is necessary for the conveyance of communications. However, the principle of confidentiality shall still apply.

Further to this, the network or service provider ("**undertaking company**") shall not be held liable for the protection of the conveyed information if such information can be directly listened to or obtained at the location of the broadcasting and/or reception.

However, this ban does not apply to temporary recording and storing of messages and related traffic data if it is required; (i) for the provision of value added services ordered by a subscriber or user; (ii) to prove a request to establish, change or withdraw the service; or (iii) to prove the existence or validity of other legal acts, which the subscriber, user or undertaking company has made.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Under the ECA, each person that stores or gains access to the information stored in the terminal equipment of a user must be authorised for such processing by the concerned user whose consent must be based upon exact and complete information regarding the purpose of such processing of the data. In this regard, also the use of the respective setting of the web browser or other computer programme is considered (implied) consent.

Traffic Data – Traffic Data can only be processed for the purpose of the conveyance of a communication on an electronic communications network or for the invoicing thereof. The Traffic Data related to subscribers or users may not be stored without the consent of the person concerned and the undertaking company is required, after the end of a communication transmission, without delay, to destroy or make anonymous, except the cases as defined by the ECA.

If it is necessary for the invoicing of the subscribers and network interconnection payments, the undertaking company is required to store the Traffic Data until the expiration of the period during which the invoice may be legally challenged or the claim for the payment may be asserted. The undertaking company is required to provide the Traffic Data to the Office or the court in case of a dispute between undertaking companies or between an undertaking company and a subscriber. The scope of the stored Traffic Data must be limited to the minimum necessary.

Location Data – The undertaking company may process the Location Data other than the Traffic Data which relates to the subscriber or the user of a public network or public service only if the data are made anonymous or the processing is done with user consent, and in the scope and time necessary for the provision of the value added service. The undertaking company must, prior to obtaining consent, inform the subscriber or user of the Location Data other than Traffic Data which will be processed, on the purpose and duration, and whether the data will be provided to a third party for the purposes of the provision of the value added service. The subscriber or user may revoke its consent for the processing of the location data at any time.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

51. SOUTH AFRICA

CONTRIBUTION DETAILS

Cliffe Dekker Hofmeyr Inc.
DLA Piper Group Member
www.cliffedekkerhofmeyr.com

Preeta Bhagattjee
Head of Data Protection and Privacy Group
T +2711 562 1038
preeta.bhagattjee@dlacdh.com

LAW

Although there is currently no data protection legislation in force:

- the Constitution of the Republic of South Africa guarantees the right to privacy;
- certain provisions within the Electronic Communications and Transactions Act regulate the electronic collection of personal information, although compliance with these provisions is voluntary; and
- the Protection of Personal Information Bill ("**PPI Bill**"), when passed as law will safeguard personal information by imposing stringent obligations on persons holding and processing personal information. The PPI Bill has been submitted for parliamentary approval. It has been approved by the National Assembly and is currently before the National Council of Provinces for deliberation. It is not currently clear when such deliberations will commence.

DEFINITION OF PERSONAL DATA

"Personal Information" is defined broadly in the PPI Bill to include information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person/legal entity and includes:

- information about a person's race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well being, disability, religion, conscience, belief, culture, language and birth;
- information relating to the education, medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about that person; and
- the name of the person, if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

DEFINITION OF SENSITIVE PERSONAL DATA

The Bill provides for a separate category of information called "Special Personal Information" which includes all information relating to a child (who is subject to parental control in terms of the law), and a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.

NATIONAL DATA PROTECTION AUTHORITY

Currently there is no authority specifically established for the purpose of data protection. This will change once the PPI Bill is passed as law, as it provides for the establishment of an independent supervisory authority, namely the Information Protection Regulator ("**Regulator**").

The Regulator is entrusted with extensive powers and duties, including the right to establish committees, promote understanding and acceptance of the information protection principles imposed by the PPI Bill, undertake educational programmes and research, examine proposed legislation, report to Parliament, conduct audits, act as mediator, receive and investigate complaints relating to alleged violations, issue codes of conduct, assist bodies in the development of codes of conduct and publish reports.

In the performance of its functions, the Regulator is obliged to have due regard to and take account of:

- the information protection principles;
- the protection of all human rights and social interests which compete with the right to privacy (including the desirability of the free flow of information);
- international obligations accepted by South Africa; and
- developing international guidelines relevant to the protection of individual privacy.

REGISTRATION

Currently there are no notification/registration requirements for the processing of data.

This position will change when the PPI Bill is enacted. The PPI Bill places an obligation on public or private bodies which alone, or in conjunction with others, determine the purpose of and means for the processing of Personal Information ("**Responsible Parties**") to notify the

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Regulator prior to the processing of personal information. The PPI Bill also prescribes the particulars which must be incorporated in any such notification, including the name and address of the responsible party, the purpose of the processing (including any trans border flows of the information), a description of the categories of data subjects, a description of the information or categories of information, and the recipients or categories of recipients to whom the personal information may be supplied. Failure to comply with the notification requirement amounts to an offence. The Regulator may exempt certain categories of information processing from the notification requirement.

The PPI Bill also provides that the Regulator is obliged to maintain a register of all information processing of which it has been notified. The register may, subject to certain exceptions, be consulted by any person free of charge.

DATA PROTECTION OFFICERS

Although there is currently no requirement for public or private bodies to appoint data protection officers, this will be impacted by the PPI Bill once passed as law. The PPI Bill provides for the appointment of Information Protection Officers in respect of both public and private bodies. The Information Protection Officers will be responsible for encouraging compliance with the provisions of the PPI Bill, dealing with any requests made to that body, and cooperating with the Regulator in respect of any investigations by the Regulator in relation to that body.

An Information Protection Officer will be obliged to assume its duties once a responsible party has registered the public or private body with the Regulator.

COLLECTION AND PROCESSING

Currently, there are no laws that regulate the collection and processing of data. The PPI Bill, once enacted as law, will significantly change this position.

The PPI Bill specifically imposes eight information protection principles or conditions, namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. These principles give effect to internationally accepted information protection principles and help ensure that the PPI Bill prescribes the minimum requirements for lawful processing of personal information. Responsible parties may process (which includes collecting) personal information where, inter alia:

- the information protection principles are met;
- the processing is performed in a reasonable manner that does not infringe the data subject's privacy and is for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;
- the data subject has been made aware of, inter alia, the nature of the information being collected, the identity of the responsible party and the purpose of the collection of the information;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- in relation to processing, such processing is adequate, relevant and not excessive;
- the data subject has consented thereto, or the processing is necessary for the conclusion of a contract, complies with an obligation imposed by law, protects a legitimate interest of the data subject, or is necessary for pursuing the legitimate interests of the responsible party or a third party to whom the information is supplied;
- the personal information is collected directly from the data subject (unless the information has been made public by the data subject, the data subject has consented to collection from another source, the data subject's interests would not be prejudiced by the collection, the collection is necessary per the grounds contemplated in the PPI Bill, the lawful purpose of the collection would be prejudiced or compliance is not reasonably practical);
- the data subject will continue to have access to the personal information (subject to certain exemptions); and
- the responsible party has taken appropriate technical and organisational measures to safeguard the security of the information.

The PPI Bill distinguishes between personal information and special personal information. The processing of special personal information by responsible parties is prohibited under the PPI Bill. The term "Special Personal Information" is discussed above. The prohibition is, however, subject to a number of exemptions.

TRANSFER

Although there is currently no regulation of the transfer of data, this will be altered by the PPI Bill once passed as law.

The PPI Bill provides that a responsible party may not transfer personal information about a data subject to a third party in a foreign jurisdiction unless:

- the recipient is subject to a law or contract which:
  - upholds principles of reasonable processing of the information that are substantially similar to the principles contained in the PPI Bill; and
  - includes provisions that are substantially similar to those contained in the PPI Bill relating to the further transfer of personal information from the recipient to third parties;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- the transfer is for the benefit of the data subject and:
  - it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
  - if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Currently, there is no law that regulates the security of processed data. The PPI Bill, once enacted as law, will significantly change this position.

Under the PPI Bill, a responsible party must secure the integrity of the personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

- loss of, damage to, or unauthorised destruction of personal information; and
- unlawful access to, or processing of, personal information.

To give effect to these measures, the responsible party must take reasonable steps to:

- identify all reasonably foreseeable internal and external risks to personal information under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

BREACH NOTIFICATION

As there is currently no effective data protection legislation in place, this does not apply. The PPI Bill, however, would require breach notification, so this position will change once the PPI Bill is passed as law.

Under the PPI Bill, where there are reasonable grounds to believe that a data subject's personal information has been accessed or acquired by an unauthorised person, the responsible party, or any third party processing personal information under the authority of the responsible party, must notify the Regulator and the data subject, unless the identity of the data subject cannot be established.

Notification to the data subject must be:

- made as soon as reasonably possible after the discovery of the breach;
- sufficiently detailed; and
- in writing and communicated to the data subject by mail (to the data subject's last known physical or postal address), email to the data subject's last known email address, placement in a prominent position on the website of the responsible party, publication in the news media, or as may be directed by the Regulator.

The notification must include such detail as to allow the data subject to take protective measures.

A responsible party may be directed by the Regulator to publicise the breach where the Regulator has reasonable grounds to believe that such publicity would protect the data subject.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

As there is currently no effective data protection legislation in place, this does not apply. The PPI Bill, however, would regulate the processing of personal information and accordingly provides for specific enforcement mechanisms which will change this position once passed as law.

The Regulator is responsible for the investigation and enforcement of the PPI Bill.

Any person may, either orally or in writing (although oral submissions are to be converted to writing as soon as reasonably practicable), submit a complaint to the Regulator in the event of alleged interference.

The PPI Bill provides that, after receipt of a complaint, the Regulator is obliged to investigate the complaint, act as a conciliator where appropriate and take further action as contemplated by the PPI Bill.

In exercising its investigative powers, the Regulator may *inter alia* administer the oath, summon and enforce the appearance of persons, compel the provision of written or oral evidence under oath, receive evidence irrespective of whether such evidence is admissible in a court of law, and enter and search any premises occupied by a responsible party. Where necessary, the Regulator may apply to a judge of the High Court or a magistrate to issue a warrant to enable the Regulator to enter and search premises.

Any person who obstructs the Regulator, breaches the confidentiality provisions contained in section 47, intentionally obstructs or unreasonably fails to assist in the execution of a warrant, or fails to comply with an information or enforcement notice is guilty of an offence and liable on conviction to a fine or imprisonment (or both) for a period of no longer than ten years in respect of the obstruction of the Regulator, or 12 months in respect of the other offences created by the PPI Bill.

Data controllers have a right of appeal against a decision of the Regulator and a data subject has the right to institute a civil action for damages in a court against a data controller for breach of any provision of the PPI Bill.

ELECTRONIC MARKETING

Currently, the Consumer Protection Act ("**CPA**") deals with the consumer's right to restrict unwanted direct marketing while the Electronic Communication and Transactions Act ("**ECTA**") regulates unsolicited electronic communications.

Under the CPA, consumers have the right to pre-emptively block any direct marketing. Any consumer who has been sent any marketing communication may demand the persons responsible for initiating the communication desist from sending any further communication to them. The ECTA has similar provisions and specifically requires that each electronic message be accompanied by an option to cancel (i.e. opt-out) a subscription to a mailing list and also requires the sender of the message to provide specific identifying information, including name and contact information.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

There is currently no regulation of electronic marketing from a data privacy perspective with regard to personal information, but this position will be altered by the PPI Bill once it comes into force.

Under the PPI Bill, data subjects have certain rights with respect to unsolicited electronic communications (i.e. direct marketing by means of automatic calling machines, facsimile machines, SMSs or emails). The processing of the data subject's personal information for the purposes of direct marketing is prohibited unless the data subject has given its consent or the email recipient is a customer of the responsible party. When sending emails to a data subject who is a customer, the responsible party must have obtained the details of the data subject through a sale of a product or service, the marketing should relate to its own similar products or services and the data subject must have been given a reasonable opportunity to object to the use of its personal information for marketing when such information was collected.

The PPI Bill also prohibits automated processing of personal information where the data subject will be subjected to a decision which has legal consequences for the data subject or which affects the data subject to a substantial degree. There are certain exceptions to this prohibition.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The PPI Bill as of the time of writing does not contain provisions regulating the use of cookies or location data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

51. SOUTH KOREA

CONTRIBUTION DETAILS

Bae, Kim and Lee LLC
www.bkl.co.kr

Kim, Kwang Jun
Partner
T +82 2 3404 0481
Kwangjun.kim@bkl.co.kr

Ryoo, Kwang Hyun
Partner
T +82 2 3404 0150
KH.Ryoo@bkl.co.kr

Kim, Ji Hyun
Partner
T +82 2 3404 0180
Jihyun.kim@bkl.co.kr

Kang, Taeuk
Partner
T +82 2 3404 0485
Taeuk.kang@bkl.co.kr

LAW

In the past, South Korea did not have a comprehensive law governing data privacy. However, a new law relating to protection of personal information (Personal Information Protection Act, "**PIPA**") was enacted and became effective as of 30 September 2011.

Moreover, there is sector specific legislation such as:

- The Act on Promotion of Information and Communication Network Utilization and Information Protection ("**IT Network Act**") which regulates the collection and use of personal information by IT Service Providers, defined as telecommunications business operators under Article 2.8 of the Telecommunications Business Act; and other persons who provide information or intermediate the provision of information for profit by utilizing services rendered by a telecommunications business operator;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- The Use and Protection of Credit Information Act ("UPCIA") which regulates the use and disclosure of Personal Credit Information, defined as credit information which is necessary to determine the credit rating, credit transaction capacity, *etc*. of an individual person. The UPCIA primarily applies to a Credit Information Providers/Users, defined under Article 2.7 of the UPCIA as a person (entity) prescribed by Presidential Decree thereof who provides any third party with credit information obtained or produced in relation to his/her own business for purposes of commercial transactions, such as financial transactions with customers, or who has been continuously supplied with credit information from any third party to use such information for his/her own business; and
- The Act on Real Name Financial Transactions and Guarantee of Secrecy ("**ARNFTGS**") which applies to information obtained by financial or financial services institutions.

Under PIPA, except as otherwise provided for in any other Act, the protection of personal information shall be governed by the provisions of PIPA.

DEFINITION OF PERSONAL DATA

Under PIPA, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, images, or other similar information (including information that does not, by itself, make it possible to identify a specific person but that which enables the recipient of the information to easily identify such person if combined with another information).

Under the IT Network Act, information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, or similar in a form of code, letter, voice, sound, image, or any other form (including information that does not, by itself, make it possible to identify a specific person but that enables to identify such person easily if combined with another information).

The relevant Korean authorities' understanding is that the construction of Personal Data under PIPA and that under IT Network Act are same in spite of subtle difference in definition wordings.

DEFINITION OF SENSITIVE PERSONAL DATA

Under PIPA, Sensitive Personal Data is defined as Personal Data consisting of information relating to a living individual's: (i) thoughts or creed; (ii) history regarding membership in a political party or labor union; (iii) political views; (iv) health care and sexual life; and (v) other Personal Data stipulated under the Enforcement Decree (the Presidential Decree) which is anticipated to otherwise intrude seriously upon the privacy of the person. The Enforcement Decree of PIPA includes genetic information and criminal record as Sensitive Personal Data. IT Network Act also has a similar definition.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

The Minister of Public Administration and Security (the "**MOPAS**") is in charge of the execution of PIPA.

The Korea Communications Commission (the "**KCC**") is in charge of the execution of the IT Network Act.

REGISTRATION

Under PIPA, a public institution which manages a Personal Data file (collection of Personal Data) shall register the following with the MOPAS: (a) name of the Personal Data file; (b) basis and purpose of operation of the Personal Data file; (c) items of Personal Data which are recorded in the Personal Data file; (d) the method to process Personal Data; (e) period to retain Personal Data; (f) person who receives Personal Data generally or repeatedly; and (g) other matters prescribed by Presidential Decree. A "public institution" in this context refers to any government agency or institution.

The Presidential Decree of PIPA stipulates that the followings also shall be registered before MOPAS:

- the name of the institution which operates the Personal Data file;
- the number of subjects of the Personal Data included in the Personal Data file;
- the department of the institution in charge of Personal Data processing;
- the department of the institution handling the Personal Data subjects' request for inspection of Personal Data; and
- the scope of Personal Data inspection of which can be restricted or rejected and the grounds therefore.

Only "public institutions" are required to register before the MOPAS.

DATA PROTECTION OFFICERS

Under PIPA, every Data Handler (which means any person, any government entity, company, individual or other person that, directly or through a third party, handles Personal Data in order to manage Personal Data files for work purposes) must to designate a data protection officer.

Under IT Network Act, every IT Service Provider must designate a director or chief officer of department in charge of handling Personal Data as a data protection officer. Pursuant to Presidential Decree of the IT Network Act to, an IT Service Provider with less than 5 employees, the owner or representative director shall be the person in charge.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

If a Data Handler under PIPA or an IT Service Provider under IT Network Act intends to collect Personal Data from the data subject or IT service user, it must:

- first notify the data subject or IT service user of the vital information stipulated under the law; and
- obtain the data subject's or IT service user's prior consent to such collection other than some exceptional cases stipulated under the law.

If a Data Handler under PIPA intends to collect Sensitive Personal Information, the consent must be separately obtained.

Under the newly amended IT Network Act, which became effective as of 18 August 2012, an IT Service Provider shall not collect a Resident Registration number (equivalent to Social Security number in the United States), unless (i) the IT Service Provider is designated as an identification institution by the KCC; or (ii) there exist special provisions under any other laws or Notification of the KCC.

Under the PIPA, prior to obtaining the prerequisite consent for collecting Personal Data from a data subject, a Data Handler must notify the data subject of (a) the purpose of collection and use of Personal Data, (b) items of Personal Data to be collected and (c) time period for possession and use of Personal Data, (d) the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, prior to obtaining prerequisite consent for collecting Personal Data from IT service user, an IT Service Provider must notify the IT service user of (a) the purpose of collection and use of Personal Data, (b) items of Personal Data to collect and (c) time period for possession and use of Personal Data.

When a certain business transfer occurs, the Data Handler or IT service provider, must provide its data subjects or IT service users a chance to opt out by providing a notice, including items of: (a) the expected occurrence of Personal Data transfers; (b) the contact information of the recipient of the Personal Data, including the name, address, telephone number and other contact details of the recipient; and (c) the means and process by which the data subject or IT service user may refuse to consent to the transfer of Personal Data.

If the data subject or IT service user is under 14, the consent of his/her legal guardian must be obtained.

As a general rule, a Data Handler under PIPA or an IT Service Provider under IT Network Act may not handle Personal Data, without obtaining the prior consent of the data subject or IT service user, beyond the scope necessary for the achievement of the Purpose of Use. This general rule also applies where a Data Handler or IT Service Provider acquires Personal Data as a result of a merger or acquisition.

Exceptions to the general rule above apply in the following cases under PIPA:

- Where there exist special provisions in any Act or it is inevitable to fulfil an obligation imposed by or under any Act and subordinate statute;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Where it is inevitable for a public institution to perform its affairs provided for in any Act and subordinate statute, etc.;
- Where it is inevitably necessary for entering into and performing a contract with a subject of Personal Data;
- Where it is deemed obviously necessary for the physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.; and
- Where it is necessary for a Data Handler to realise his/her legitimate interests and this obviously takes precedence over the rights of a subject of Personal Data. In such cases, this shall be limited to cases where such data is substantially relevant to a Data Handler's legitimate interests and reasonable scope is not exceeded.

Exceptions to the general the rule above apply in the following cases under IT Network Act:

- If the Personal Data is necessary in performing the contract on provision of IT services, but it is obviously difficult to get consent in an ordinary way due to any economic or technical reason;
- If it is necessary in settling the payment for charges on the IT services rendered; and
- If a specific provision exists in this Act or any other Act.

Under the ARNFTGS, financial institutions must obtain written consent for the disclosure of an individual's information relating to his/her financial transactions.

TRANSFER

As a general rule, a Data Handler or an IT Service Provider may not provide Personal Data to a third party without obtaining the prior opt in consent of the data subject or IT service user.

Exceptions to the general rule above apply in the following cases under PIPA:

- Where there exist special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute;
- Where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc.; and
- Where it is deemed obviously necessary for physical safety and property interests of a subject of Personal Data or a third person when the subject of Personal Data or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.

Exceptions to the general rule above apply under IT Network Act if a specific provision exists in this Act or any other act otherwise.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Under PIPA, a Data Handler must obtain consent after it notifies the data subject of (a) the person (entity) to whom the Personal Data is furnished, (b) purpose of use of the Personal Data by the person (entity), (c) types of Personal Data furnished, (d) period of time during which the person (entity) will possess and use the Personal Data and (e) the fact that the data subject has the right to refuse to consent and the consequences of refusing.

Under the IT Network Act, an IT Service Provider must notify the IT service user of (a) the person (entity) to whom the Personal Data is furnished, (b) purpose of use of the Personal Data by the person (entity), (c) types of Personal Data furnished and (d) period of time during which the person (entity) will possess and use the Personal Data, and then obtain consent from the IT service user.

The UPCIA stipulates that prior to obtaining prerequisite consent for providing personal credit information to any other person, a Credit Information Provider/User must notify the credit information subject of (a) the person (entity) to whom the credit information will be furnished;(b) the purpose of use of the Personal Credit Information by the person (entity); (c) the types of Personal Credit Information to be furnished; and (d) the period of time during which the person (entity) will possess and use the Personal Credit Information.

Exceptions to the general rule above apply in the following cases under the UPCIA:

- Where a Credit Information Company as defined under the Article 2.5 of the UPCIA provides such information for the purpose of performing central management and utilization thereof with another Credit Information Company or Credit Information Collection Agency as defined under the Article 2.6 of the UPCIA;
- Where such provision is required to perform a contract, and to entrust the processing of credit information under Article 17.2 of the UPCIA;
- Where the relevant Personal Credit Information is provided as part of rights and obligations that are transferred by way of business transfer, division, merger, etc.;
- Where Personal Credit Information is provided for a person who uses the information for purposes prescribed by Presidential Decree, including claims collection (applicable only to the credit which is an object of collection), license and authorization, determination of a company's credit worthiness, and transfer of securities;
- Where Personal Credit Information is provided in accordance with a court order for submission thereof or a warrant issued by a judicial officer;
- Where such information is provided upon the request of a prosecutor or judicial police officer, in the event of occurrence of an emergency where a victim's life is in danger or he/she is expected to suffer bodily injury, etc., so that no time is available to issue a judicial warrant;
- Where such information is provided as the head of a competent government office requests, in writing, for the purpose of inquiry and examination in accordance with any laws pertaining to taxes or demands the taxation data required to be provided in accordance with such laws pertaining to taxes;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- Where Personal Credit Information held by a financial institution is provided to a foreign financial supervisory body in accordance with international conventions, etc.; and
- Where such information is otherwise provided in accordance with other laws.

Under the ARNFTGS, financial institutions must obtain written consent for the transfer of an individual's information relating to his/her financial transactions to a third party.

SECURITY

Under PIPA and IT Network Act, every Data Handler or IT Service Provider must, when it handles Personal Data of data subject or IT service user, take the following technical and administrative measures in accordance with the guidelines prescribed by Presidential Decree to prevent loss, theft, leakage, alteration, or destruction of Personal Data:

- establishment and implementation of an internal control plan for handling Personal Data in a safe way;
- installation and operation of an access control device, such as a system for blocking intrusion to cut off illegal access to Personal Data;
- measures for preventing fabrication and alteration of access records;
- measures for security including encryption technology and other methods for safe storage and transmission of Personal Data;
- measures for preventing intrusion of computer viruses, including installation and operation of vaccine software; and
- other protective measures necessary for securing the safety of Personal Data.

BREACH NOTIFICATION

Under PIPA, if a breach of Personal Data occurs the Data Handler must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects exceeds 10,000, the Data Handler shall immediately report the notification to data subjects and the result of measures taken to MOPAS, KISA or the National Information Security Agency (the "**NIA**").

Under the IT Network Act, an IT Service Provider must, if it discovers an occurrence of intrusion:

- immediately report it to the KCC or the Korea Internet & Security Agency (the "**KISA**"); and
- analyse causes of intrusion and prevent damage from being spread, whenever an intrusion occurs.

The KCC may, if deemed necessary for analyzing causes of an intrusion, order an IT Service Provider to preserve relevant data, such as access records of the relevant information and communications network.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Under the newly amended IT Network Act, which became effective as of 18 August 2012, if a loss, theft or leakage of Personal Data occurs, the IT Service Provider must notify the IT Service user and report to the KCC without delay of the details and circumstances, and the remedial steps planned.

ENFORCEMENT

The competent authorities may request reports on the handling of Personal Data, and also may issue recommendations or orders if a Data Handler or IT Service Provider violates PIPA or the IT Network Act. Non compliance with a request or violation of an order can result in fines, imprisonment, or both.

For example, MOPAS, the supervising authority for Data Handler, can issue a corrective order in response to any breach of an obligation not to provide Personal Data to a third party. Breach of a corrective order leads to an administrative fine of not more than KRW 30 million. Prior to issuing a corrective order, MOPAS may take an incremental approach and instruct, advise and make recommendations to the Data Handler.

Under the IT Network Act, an IT Service Provider who collected Personal Data without consent of the relevant user shall be subject to the penalty of imprisonment for not more than 5 years or a fine not exceeding KRW 50 million.

Under the UPCIA, a Credit Information Provider/User who has provided Personal Credit Information without consent of the relevant credit information subject shall be subject to the penalty of imprisonment of up to 5 years or a fine not exceeding KRW 50 million.

Under the ARNFTGS, a person who discloses information or data concerning financial transactions shall be punished by imprisonment not exceeding 5 years or by a fine not exceeding KRW 30 million.

ELECTRONIC MARKETING

The transmission of an advertisement via an information and communication network, including electronic mails is not prohibited by the IT Network Act, but provides individuals with the right to prevent the processing of their personal data (e.g. a right to "opt out") for electronic marketing purposes. An IT Service Provider who intends to transmit an advertisement by information and communication network must specify the following information in the advertisement.

- The type and main contents of the transmitted information;
- The name and contact information of the sender;
- The source from which the electronic mail address was collected (applicable only when transmitted by electronic mail); and
- Matters concerning the measures and method by which the addressee can express his intention to decline reception of the information easily.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

A person who intends to transmit an advertisement by telephone (includes SMS text messages) or facsimile shall obtain a prior consent (e.g. a right to "opt in") from the addressee, unless (a) the person who has collected an addressee's contact information directly through a transaction of goods, etc. intends to transmit to the addressee any advertising information for profit concerning the goods, etc. offered by that person or (b) the relevant advertising information falls under the definition of an advertisement under the Act on the Consumer Protection in the Electronic Commerce Transactions, etc. or a soliciting telephone call under the Door-to-Door Sales, etc. Act. A person who intends to transmit an advertisement by telephone or facsimile must specify the following information.

- The name and contact information of the sender; and
- Matters concerning the measures and method by which the recipient can express his intention to revoke his consent to receive the information easily.

A person who transmits an advertisement shall not take any of the following technical measures.

- A measure to avoid or impede the addressee's denial of reception of the advertising information or the revocation of his consent to receive such information;
- A measure to generate an addressee's contact information, such as telephone number and electronic mail address, automatically by combining figures, codes, or letters;
- A measure to register electronic mail addresses automatically with intent to transmit advertising information for profit; and
- Various measures to hide the identity of the sender of advertising information or the source of transmission of an advertisement.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookie, log, IP information, etc. are also regulated by the IT Network Act as personal data, which if combined with other information enable the identification a specific individual person easily. Under the IT Network Act, using cookies (or web beacons) must be done with the opt-out consent of the user and the privacy policy must publicise the matters concerning installation, operation and opt-out process for automated means of collecting personal information, such as cookies, logs and web beacons.

The protection of location information is governed by the provisions of the Act on the Protection, Use, etc. of Location Information (the "**LBS Act**").

Under the LBS Act, any person who intends to collect, use, or provide location information of a person or mobile object shall obtain the prior consent of the person or the owner of the object, unless (a) where there is a request for emergency relief or the issuance of a warning by an emergency rescue and relief agency; (b) where there is a request by a police for the rescue of the person whose life or physical safety is in immediate danger; or (c) where there exist special provisions in any Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Under the LBS Act, any person (entity) who intends to provide services based on location information (the "**Location-based Service Provider**") shall report to the KCC. Further, any person (entity) who intends to collect location information and provide the collected location information to location-based service providers (the "**Location Information Provider**") shall obtain a license from the KCC.

If a Location Information Provider intends to collect personal location information, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information.

- Name, address, phone number and other contact information of the Location Information Provider;
- Rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- Details of the services the Location Information Provider intends to provide to Location-based Service Providers;
- Grounds for and period of retaining data confirming the collection of location information; and
- Methods of collecting location information.

If a Location-based Service Provider intends to provide location-based service by utilising personal location information provided from Location Information Provider, it must specify the following information in its service agreement, and obtain the consent of the subjects of personal location information;

- Name, address, phone number and other contact information of the Location-based Service Provider;
- Rights held by the subjects of personal location information and their legal agents and methods of exercising the rights;
- Details of the Location-based Services;
- Grounds for and period of retaining data confirming the use and provision of location information; and
- Matters concerning notifying the personal location information subject of the provision of location information to a third party as below.

If a Location-based Service Provider intends to provide location information to a third party, in addition to the above, it must notify the subjects of personal location information of the third party who will receive the location information and the purpose of this provision.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

52. SPAIN

CONTRIBUTION DETAILS

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

LAW

As a member of the European Union, Spain formally implemented the EU Data Protection Directive 95/46/EC in November 1999 with the Special Data Protection Act 1999 (the "**Act**", also known as the "**LOPD**" in Spain). Nevertheless, from 1992, Spain already had a Data Protection Act ("**LORTAD**") that was fully consistent with most of the contents of the EU Data Protection Directive 95/46/EC. The Act, simply represents an up-to-date version of LORTAD, rather than being a major change in the legal framework. Enforcement is through the Spanish Data Protection Commissioner's Office ("**AEPD**"). Its last amendment took place in March 2011.

DEFINITION OF PERSONAL DATA

Any information (including numbers, text, graphics, pictures, video, sounds or any other type of data) related to individuals that are identified or identifiable.

DEFINITION OF SENSITIVE PERSONAL DATA

Personal data related to political orientation, religion, beliefs, trade union membership, ethnic origin, health and sex life. Each category of sensitive information enjoys, however, a different level of protection. Of note, criminal/administrative infringements data can be included only in the databases of certain public authorities and companies, with individuals being forbidden to do so, whilst other categories allow collection and processing under certain conditions.

NATIONAL DATA PROTECTION AUTHORITY

The Spanish Data Protection Commissioner's Office ("**AEPD**", standing in Spanish for "Agencia Española de Protección de Datos"). It is based in Madrid. Regional commissioners exist as well in certain territories, dealing only with data protection issues of the regional public authorities themselves.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

Unlike other EU Member States, Spain does not maintain a register of controllers or of processing activities. Instead, the AEPD holds a registry of databases containing personal information. Registration, carried out through state of the art software provided by the AEPD (called NOTA), is very detailed and identifies in full not only the data controller, but also any data processors supporting it. It contains a clear description of the database contents, the sources of the data, the purposes for which the data is collected, processed and transferred, as well as the identity of the recipients of the information, with special attention paid to international transfers. Any changes to the database require the registration to be amended.

DATA PROTECTION OFFICERS

Although there is no blanket requirement in Spain for organisations to appoint a data protection officer as such, organisations handling personal information to which "medium" or "high" security requirements apply shall appoint a Head of Data Security. The Head of Data Security is not in charge of data protection matters in general, but only the security measures to be applied to databases.

COLLECTION AND PROCESSING

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

- the data subject consents;
- the data controller needs to process the data to enter into or carry out a contract or pre contractual deal to which the data subject is a party so that the contract or deal can be maintained or executed;
- the data is collected from "public open sources" and the processing is necessary to satisfy a legitimate interest of the data controller or a third party receiving the data, provided that the constitutional basic rights of the data subject are preserved;
- the processing protects the data controller's vital interests; or
- the processing is required by an enactment or to legitimately perform a public function in the public interest.

Where sensitive personal data is processed, one of the above conditions must be met plus one further condition from a separate list of more stringent conditions (explicit and written consent in the case of political, moral and religious beliefs and trade union membership or explicit consent from the data subject plus general interest grounds supported by a law, in the case of ethnic origin, health and sex life).

Whichever of the above conditions is relied upon, the data controller must provide the data subject with "fair processing information". This includes the existence of a database storing his/her personal data, the identity and address of the data controller, the purposes of processing, the consequences of supplying/refusing to supply the information, whether it is mandatory or not to supply the information requested, and how the data subject may exercise the rights of access, modification, cancellation and objection to the data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

Data controllers may transfer personal data to third parties (group companies being considered third parties for this purpose) if any of the following conditions are met:

- the data subject consents;
- the transfer is endorsed by a law;
- the data is collected from "public open sources";
- the transfer to a third party is essential to a contract to which the data subject has become freely and legitimately a party;
- the transfer is intended for the national or regional Ombudsman ("**Defensor del Pueblo**"), Public Prosecutor, Judges and Courts, and the Public Finances Court, within their legal faculties;
- the transfer takes place between public bodies and is intended for historical, statistical or scientific research; or
- the transfer is urgently needed to protect the health of the data subject or other individuals.

Consent can be revoked at any time and will be void if the information provided to the data subject did not allow them to determine the purposes for which the data should be used, or the scope of the activities of the recipient.

These principles apply to transfers within Spain or within the European Economic Area. Transfers of a data subject's personal data to non EU/European Economic Area countries is similarly allowed under the following circumstances: those countries provide "adequate protection" for the security of the data (e.g. Argentina); if the transfer takes place under a Treaty to which Spain is a party; if it is intended to provide or to request international judiciary cooperation; if the transfer is required for serious medical matters, if it refers to international money transfers; if the data subject consents to it in a unequivocal manner; if the transfer is necessary to execute a contract or a pre-contractual deal between the data subject and the data controller upon a request of the former; if the transfer is necessary to execute, in the interests of the data subject, a contract between the data controller and a third party; if the transfer is necessary to protect a public interest; if the transfer is necessary for the enforcement, exercise or defence of a right at court; or if the transfer takes place from a Public Registry for a legitimate purpose and to a legitimate recipient, following the instructions of a legitimated person.

In any other case, the transfer abroad to non-adequate territories must be authorised in advance by the AEPD (the use of "standard contractual clauses" approved by the European Commission, or the implementation of Binding Corporate Rules easing the granting of such approval).

For the transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of the AEPD. Consent clauses, however, are deemed valid only if they explicitly mention that the recipient is based in the US and that data protection laws there do not offer a level of privacy protection equivalent to that applied within the EU.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Data controllers and processors must take appropriate technical and organisational measures against unauthorised or unlawful access or processing, and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the nature of the data. "Basic" security measures must be applied to all data, and include, inter alia, control of access to data by employees of the data controller. "Medium" security measures must be applied to data relating to financial services, public security, public tax matters or which may allow data controllers to profile a data subject in detail. These measures include, inter alia, the execution of privacy audits every two years and the appointment of a Head of Data Security. Databases containing sensitive information (as well as data relating to gender violence, and police records) require "high" security measures, including, inter alia, tougher access control and data encryption when communicating the data.

BREACH NOTIFICATION

As of yet, there is no mandatory requirement in the LOPD to report data security breaches or losses to the AEPD or to data subjects. Nevertheless, the organisation is required to record such incidents in the Security Incidents Ledger. The AEPD is entitled to request to see the Security Incidents Ledger at any time. As a matter of fact, Police Forces and Public Offices do normally immediately report to the AEPD any data breach or loss of personal data they may be informed about (e.g. when a claim for the theft of a hard disk is filed by the owner). In March 2012, the Spanish General Telecommunications Act was amended to oblige telecommunications operators to rapidly report data breaches to AEPD and to the relevant data subjects. Rumours on the possibility of extending that obligation to other companies have been heard, but this has not happend to date.

ENFORCEMENT

In Spain, the AEPD is responsible for enforcement of the Act. Acting either ex officio or upon a complaint from a data subject (or a public authority, for example the Consumer Protection Office to which the data subject has complained), the AEPD is entitled to start:

- an investigation procedure, to collect information;
- a privacy rights protection procedure, when a data controller is refusing to allow a data subject to exercise his/her access, rectification, cancellation or objection rights; and
- a disciplinary procedure when enough evidence has been gathered to suspect that a data controller has infringed the LOPD.

Notably, the AEPD does not issue any "warnings" to the data controllers asking them to comply with the law. The first notice that, an organisation may receive from the AEPD is the commencement of a disciplinary procedure. As data protection rights are constitutional rights in Spain, negligence or error are not commonly considered as a reason to mitigate the sanction.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Sanctions are essentially monetary fines. They range from EUR 900 to EUR 40,000 for minor infringements, EUR 40,001 to EUR 300,000 for serious infringements and EUR 300,001 to EUR 600,000 for very serious infringements. Very serious and serious infringements are more frequently detected and sanctioned than minor ones. The fines stated here are per infringement, but very often fines are aggregated within a given case to form a larger total fine.

ELECTRONIC MARKETING

Electronic Marketing is regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce ("**LSSI**"), as amended in March 2012. The general principle is that deliveries of electronic marketing materials are lawful only if they have been explicitly authorised in advance by the recipients (authorisation that is required not just for individuals, but also when the recipient is a legal entity, broadening here the scope of Spanish Data Protection Act). An exception to this general principle applies to deliveries to clients when the materials refer to products/services that are equal or similar to the ones sold to them in the past by the company sponsoring the advertisement.

Electronic publicity shall (i) be clearly marked as such by means of the terms PUBLI or PUBLICIDAD placed inside the subject line, (ii) shall allow the recipient to opt-out at all times, even by the time of registration, and (iii) shall clearly identify the sponsor of the delivery. It is the sponsor of the delivery, not the electronic publicity company that shall be held liable in case of enforcement. Opt-out shall include an email address when the publicity was delivered by email too. Opt-out procedure shall be simple and free for the recipient of the publicity.

Enforcement shall include, inter alia, fines that, in most cases, shall be between EUR 30,000 and EUR 150,000.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookies are regulated in Spain, in addition to the Spanish Data Protection Act, by the Spanish Act on the Information Society Services and e-Commerce ("**LSSI**"), as amended in March 2012.

The new regulation requires data controllers to inform cookies' recipients (referred to in the LSSI as giving users the "actual opportunity") – including legal entities – of the existence and use of cookies, their scope and how to deactivate them. Actual opportunity is interpreted by the regulator as a procedure by which the user cannot browse the website, for example, without noticing the invitation to review the above-mentioned information and carrying out an active behaviour (even a simple one like pressing the ESC key) to continue browsing after being presented with the information or the opportunity to review it. A semi-transparent layer on the usual homepage screen is a generally approved mechanism to request the consent. Certain types of cookies (e.g. session cookies) are exempt from these restrictions as per the WP29 criteria released during the summer of 2012. The Spanish AEPD has made known to the public, by the way of a resolution, that in some cases the delivery of cookies to the computer of a user based in Spain may trigger the application of Spanish Data Protection Act in full.

On location data, the local position is that it may be acceptable provided that (i) users are informed at all times on whether the location system is active, (ii) users have agreed to be located and (iii) users have the option (especially when being off-duty if the location data is used in an employment context) to turn off the system.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

53. SWEDEN

CONTRIBUTION DETAILS

Johan Sundberg
Advokat/Partner
T +46 8 769 79 30
johan.sundberg@dlanordic.se

Johan Sundkvist
Jur. kand/Associate
T +46 8 769 79 30
johan.sundkvist@dlanordic.se

LAW

Being a member of the European Union, Sweden implemented the EU Data Protection Directive 95/46/EC in 1998 with the Personal Data Act (Sw. personuppgiftslagen, SFS 1998:204, below "**the Act**"). The previous Swedish Data Act enacted in 1973 had by then already been considered to be outdated for many years.

DEFINITION OF PERSONAL DATA

Personal data means all kinds of information that is directly or indirectly referable to a natural living person.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data means personal data that discloses race or ethnic origin, political opinions, religious or philosophical convictions and membership of trade unions. Personal data relating to health or sexual life is also embraced by the term.

NATIONAL DATA PROTECTION AUTHORITY

The Data Inspection Board (Sw. *Datainspektionen*, below "**DIB**") is the supervisory authority under the Act.

Contact details:

Datainspektionen
Drottninggatan 29, plan 5
Box 8114
104 20 Stockholm
T +46 8 657 61 00
datainspektionen@datainspektionen.se

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

REGISTRATION

All controllers except those whose processing falls under any of the exemptions in the Act, need to file notifications with the DIB.

Notification is **not** required if:

- the controller has appointed a personal data representative (a data protection officer or "Privacy Officer") and notified the DPA about this, or
- the processing would probably not result in an improper intrusion of personal integrity, if specified in rules issued by either the Government or the DIB (for instance processing of personal data in running text, processing takes place with the individuals consent, or the data relates to a registered person who has a link to the controller such as members, employees, customers).

DATA PROTECTION OFFICERS

There is no requirement in Sweden for organisations to appoint a data protection officer. It is a voluntary arrangement. However, if a data protection officer has been appointed and notified to the DIB, the general notification obligation does not apply. Instead, the officer has to maintain a register of the processing that the data controller implements and which would have been subject to the notification duty if the data protection officer had not existed.

COLLECTION AND PROCESSING

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

- the data subject consents;
- there is statutory authority for the processing;
- the processing is necessary to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract;
- the processing is necessary to enable the controller to fulfil a legal obligation;
- the processing is necessary to protect the vital interests of the data subject;
- the processing is necessary to perform a task in the public interest;
- the processing is necessary to exercise official authority; or
- to satisfy a purpose that concerns a justified interest on the part of the controller or on the part of a third party to whom the personal data is disclosed, provided that this interest outweighs the registered person's interest in protection against violation of personal integrity.

In relation to processing of sensitive personal data, additional requirements apply apart from what has been mentioned above.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Whichever of the above conditions is relied upon, the controller must first provide the data subject with certain information, unless an exemption applies. The notification shall include information on the identity of the controller, the purposes of the processing, whether the data will be disclosed and/or transferred and to who/where, the fact that the provision of data is voluntary and any other circumstances that will enable the data subject to exercise his/her rights pursuant to the Act.

TRANSFER

In principle, it is forbidden to transfer personal data that is being processed to a country outside the EU/EEA that does not have an adequate level of protection for personal data.

Even if the third country in question does not have an adequate level of protection, it is allowed to transfer personal data to such country if the registered person has given his/her consent to the transfer or when the transfer is necessary in order that:

- a contract between the registered person and the controller may be performed or measures that the registered person requested may be taken before a contract is made;
- a contract between the controller and a third party that is in the interests of the registered person may be made or performed;
- legal claims should be established, exercised or defended; or
- vital interests of the registered person may be protected.

It is also permitted to transfer personal data for use solely in a state that has acceded to the Council of Europe Convention of 28 January 1981 on the protection of individuals in automatic data processing.

Transfer of personal data to third countries is allowed if the countries provide "adequate protection" for the security of the data, or if the transfer is covered by standard contractual clauses approved by the European Commission, or subject to an organisation's Binding Corporate Rules.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles satisfies the requirements of Sweden's transfer law.

SECURITY

The data controller is liable to implement technical and organisational measures to protect the personal data. The measures shall attain a suitable level of security. When the controller engages a data assistant to conduct the processing of personal data (data processor), there shall be a written contract that specifically regulates the security aspects. The controller shall also be responsible to ensure that the assistant actually implements the necessary security measures.

It is the controller who is responsible in relation to the registered person as regards the processing, even if an assistant/processor has been engaged or if someone who works for the controller has wrongfully disclosed personal data.

The DIB may issue decisions on security measures in individual cases.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the DIB. Data security breaches are handled on a case-by-case basis and addressed by the DIB only if they for instance relate to a large number of data subjects or indicate a general non-compliance issue. There is no DIB guidance on the subject matter.

However, pursuant to the implementation of the ePrivacy Directive as amended, regarding security breach notification obligations, chapter 6 of the Swedish Electronic Communications Act (*Sw. lag om elektronisk kommunikation*, SFS 2003:389) as of July 2011 provides that a provider of publicly available electronic communications services shall without undue delay notify the Swedish Post and Telecom Authority (*Sw. Post och Telestyrelsen*) regarding privacy incidents. Where the incident is likely to adversely affect subscribers or user of whom the processed data concerns, or where the Post and Telecom Authority requests it, the provider shall also notify subscribers without undue delay. Incidents that only have a marginal effect on subscribers and users do not have to be notified to the authority. Moreover, notification is not required where the service provider has implemented appropriate security measures which renders the data unreadable to unauthorised persons.

ENFORCEMENT

The DIB has, in its capacity as the supervisory authority, the right of access to the personal data processed and information about and the documentation of processing, and is also empowered to enter premises connected with the processing.

Appeal may be made against a decision by the DIB to a general administrative court; i.e. in the first instance the County Administrative Court. The DIB may decide that a decision should apply even if it is appealed against.

A person who has intentionally or by gross negligence disclosed untrue data under the Act, who in contravention of the regulations processes sensitive personal data or data concerning offences, etc., or transfers personal data to a third country or neglects to give notice concerning the processing to the supervisory authority may be sentenced to a fine or imprisonment of at most six months. If the offence is grave, the penalty may be imprisonment up to two years. A sentence shall not be imposed in petty cases.

Furthermore, the controller may also be liable to pay compensation to a registered person for damage and violation of personal integrity caused by the processing of personal data in contravention of the Act.

ELECTRONIC MARKETING

The Act applies to most electronic marketing activities, given that it is likely that such marketing involves processing of personal data (e.g. an e-mail address is likely regarded as personal data under the Act). Please note that if the data subject's e-mail address has not been obtained in the context of a customer relationship or similar, the data subject's consent is, as a main rule, required for electronic marketing. Moreover, a data subject has a right to at any time oppose ("opt-out" of) further processing of his or her personal data for marketing purposes.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Pursuant to the Swedish Electronic Communications Act (as amended by e-Privacy Directive 2009/12/EC), a cookie may be stored on a user's terminal equipment, only if the user has been given access to information on the purpose of the processing and given his or her consent, i.e. the user must give his/her prior "opt-in" consent before a cookie is placed on the user's computer. The government stated in the preparatory works to the Swedish Electronic Communications Act that the implementation of the new e-Privacy Directive should not be regarded as a material change. This has been construed by some that implied consent through browser settings shall be regarded as a valid consent under the Act, provided that sufficient information is given to the user e.g. in a cookie policy. This is, however, unclear and the Swedish Post and Telecom Authority has not issued any guidance in this regard.

Consent is, however, not required for cookies that are;

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

Wilful or negligent breach of the Swedish Electronic Communications Act in this regard is sanctioned with fines, provided that the offense is not sanctioned by the Swedish Criminal Code (*Sw. brottsbalken*). However, if the breach is deemed to be minor, no sanction shall be imposed. To our knowledge there has been no case where a website operator has been fined for breach of the Swedish Electronic Communications Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

54. SWITZERLAND

CONTRIBUTION DETAILS

Schellenberg Wittmer
www.swlegal.ch

Christine Beusch-Liggenstorfer
Of Counsel/Attorney at Law
T +41 (0)44 215 5272
christine.beusch@swlegal.ch

Nadin Schwibs
Associate/Attorney at Law
T +41 (0)44 215 9335
nadin.schwibs@swlegal.ch

LAW

The processing of personal data is mainly regulated by the Federal Act on Data Protection of 19 June 1992 ("**DPA**") and its ordinances, i.e. the Ordinance to the Federal Act on Data Protection ("**DPO**") and the Ordinance on Data Protection Certification ("**ODPC**").

In addition, the processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

DEFINITION OF PERSONAL DATA

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

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive personal data is defined as data on:

- religious, ideological, political or trade union related views or activities;
- health, the intimate sphere or racial origin;
- social security measures; and
- administrative or criminal proceedings and sanctions.

"Personality profiles" are protected to the same extent under the DPA as sensitive personal data. Personality profiles are collections of data that allow the appraisal of essential characteristics of the personality of an individual.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Federal Data Protection and Information Commissioner (**"FDPIC"**)

Feldeggweg 1
CH 3003 Berne
Switzerland
T +41 (0)31 322 43 95
F +41 (0)31 325 99 96

The FDPIC supervises federal and private bodies, advises and comments on the legal provisions on data protection and assists federal and cantonal authorities in the field of data protection.

The FDPIC informs the public about his findings and recommendations, and maintains and publishes the register for data files.

REGISTRATION

The processing of personal data by private persons does not usually have to be notified or registered, respectively. However, private persons must register their data files before the data files are opened, if:

- they regularly process sensitive personal data or personality profiles; or
- they regularly disclose personal data to third parties;

and unless one of following exemptions applies;

- the data is processed pursuant to a statutory obligation;
- the Swiss Federal Council has exempted the particular processing from the registration requirement because it does not prejudice the rights of the data subjects;
- the data controller uses the data exclusively for publication in the edited section of a periodically published medium and does not pass on any data to third parties without informing the data subjects;
- the data is processed by journalists who use the data file exclusively as a personal work aid;
- the data controller has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files; or
- the data controller has acquired a data protection quality mark under a certification procedure according to Article 11 DPA and has notified the FDPIC of the result of the evaluation.

DATA PROTECTION OFFICERS

There is no requirement under Swiss data protection law to appoint a data protection officer.

However, a data controller can be dispensed from registering its data files if it has designated a data protection officer who:

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- carries out his/her duties autonomously and independently, i.e. without being subject to instructions;
- has a certain level of expertise that is appropriate for the relevant data processing at the company (whereas it is not relevant if the respective expertise was not acquired in Switzerland);
- must check and audit the processing of personal data within the company;
- must be in a position to recommend corrective measures when detecting any breaches of applicable data protection rules;
- must have access to all data files and all data processing within the company as well as to all other information that he/she requires to fulfill his/her duties;
- must maintain records of all data files controlled by the company and provide this list to the FDPIC or affected data subjects upon request;
- may not carry out any other activities that are incompatible with his/her duties as data protection officer.

The data controller must notify the FDPIC of the appointment of a data protection officer to be listed on the public list of companies exempted from the requirement to register their data files.

COLLECTION AND PROCESSING

The following principles apply to the collection and processing of personal data (including data of legal entities):

- personal data may only be processed lawfully, in good faith and according to the principle of proportionality;
- the collection of personal data and, in particular, the purpose of its processing must be evident to the data subject;
- personal data should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, or provided for by law;
- the data controller and any processor must ensure that the data processed is accurate;
- personal data must not be transferred abroad if the privacy of the data subject may be seriously endangered (see below);
- personal data must be protected from unauthorised processing by appropriate technical and organisational measures;
- personal data must not be processed against the explicit will of the data subject, unless this is justified by:
  - the consent of the data subject (which must be given voluntarily and based upon adequate information);
  - an overriding private or public interest; or
  - law;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- sensitive personal data or personality files must not be disclosed to a third party, unless this is justified by:
  - the consent of the data subject (which must be given expressly in addition to the voluntariness and adequate information requirement);
  - an overriding private or public interest; or
  - law.

TRANSFER

Personal data may be disclosed outside Switzerland if the destination country offers an adequate level of data protection. The FDPIC maintains and publishes a list of such countries.

The FDPIC deems the data protection legislation of all EU and EEA countries to be adequate with regard to personal data of individuals. With regard to personal data of legal entities, only a few EU countries, such as Austria, Italy and Liechtenstein, provide an adequate level of data protection.

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:

- sufficient safeguards, such as data transfer agreements or other contractual clauses, ensure an adequate level of protection abroad. These agreements or other safeguards must be notified to the FDPIC; to the extent that model clauses recognised by the FDPIC are used, mere information is sufficient;
- there are binding corporate rules that ensure an adequate level of data protection in cross border data flows within a single legal entity or a group of companies, e.g. the US Swiss Safe Harbor Framework (which mirrors the US EU Safe Harbor Framework). Such rules must be notified to the FDPIC;
- the data subject consents to the particular data export (consent must be given for each individual case, a generic consent is not sufficient);
- the processing is directly connected with the conclusion or performance of a contract with the data subject;
- disclosure is essential in order to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal rights before the courts;
- disclosure is required in order to protect the life or the physical integrity of the data subject; or
- the data subject has made the personal data publicly accessible and has not expressly prohibited its processing.

SECURITY

The data controller and any processor must take adequate technical and organisational measures to protect personal data against unauthorised processing and ensure its confidentiality, availability and integrity. In particular, personal data shall be protected against the following risks:

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- unauthorised or accidental destruction;
- accidental loss;
- technical errors;
- forgery, theft or unlawful use; and
- unauthorised altering, copying, accessing or other unauthorised processing.

The technical and organisational measures must be appropriate, in particular with regard to the purposes of the data processing, the scope and manner of the data processing, the risks for the data subjects and the current technological standards.

BREACH NOTIFICATION

There is no mandatory requirement to notify the FDPIC of any breach of the obligations under the DPA.

ENFORCEMENT

The FDPIC does not have specific direct powers to enforce the DPA. He may investigate cases on his own initiative or at the request of a third party and may issue recommendations that the method of processing be changed or abandoned. If the FDPIC's recommendation is not complied with, he may refer the matter to the Swiss Federal Administrative Court for a decision.

Furthermore, the DPA provides for criminal liability and fines of up to CHF 10,000 if a private person intentionally fails to comply with the following obligations under the DPA:

- duty to provide information when collecting sensitive data and personality profiles;
- duty to safeguard the data subject's right to information;
- obligation to notify the FDPIC with regard to contractual clauses or binding corporate rules in connection with the data transfer abroad;
- obligation to register data files; or
- duty to cooperate in an FDPIC investigation.

Criminal proceedings must be initiated by the competent cantonal prosecution authority.

Finally, under Swiss civil law the data subject may apply for injunctive relief and may file a claim for damages as well as satisfaction and/or surrender of profits based on the infringement of its privacy.

ELECTRONIC MARKETING

Electronic marketing practices must comply with the provisions of the Swiss Federal Act against Unfair Competition ("**UCA**").

With regard to the sending of unsolicited automated mass advertisement (which, in addition to emails, includes SMS, automated calls and fax messages) the UCA generally requires prior consent by the recipient, i.e. *opt-in*. As an exception, mass advertisings may be sent without

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

the consent of the recipient if the sender received the contact information in the course of a sale of his products or services, the recipient was given the opportunity to refuse the use of his/her contact information upon collection and the mass advertising relates to similar products or services of the sender.

In addition, mass advertising emails must contain the sender's correct name, address and email contact and must provide for an easy-access and free of charge *opt-out*.

The UCA generally applies to business-consumer relationships as well as to business-business relationships, i.e., mass advertisements sent to individuals and to corporations are subject to the same rules.

In principle, direct marketing by telephone is lawful in Switzerland as long as it is not done in an aggressive way (e.g. by repeatedly calling the same person). Moreover, art. 3 para. 1 lit. u UCA prohibits direct marketing by telephone to people who wish to not receive commercial communication and expressed that wish (i.e. opted-out) by marking their entry in the telephone book (e.g. through an asterisk next to a person's entry).

In addition to the rules of the UCA, the general data protection principles under the DTA also apply with regard to electronic marketing activities, e.g. the collection and maintenance of email addresses or processing of any other personal data.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

In general, the processing of personal data in the context of online services is subject to the general rules pertaining to the collection of personal data under the DPA. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is also subject to the Swiss Telecommunications Act ("**TCA**").

Under the TCA, the use of cookies is considered to be processing of data on external equipment, e.g. someone else's computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, e.g. by configuring their web browser to reject cookies.

In addition, the general rules under the DPA apply where cookies collect data related to identified or identifiable persons, i.e., personal data. The collection of personal data through cookies as well as the purpose of such a collection must be evident to the data subject. Further, the personal data collected may only be processed for the purpose (i) indicated at the time of collection, (ii) that is evident from the circumstances, or (iii) that is provided for by law.

Where the personal data collected through a cookie is (i) considered sensitive data, e.g. data regarding religious, ideological, political views or activities, or (ii) is so comprehensive that it forms a personality profile, i.e. permits an assessment of essential characteristics of the personality of a person, the stricter rules pertaining to the processing of sensitive personal data are applicable. These stricter rules provide, inter alia, that the data subject must be informed of (i) the identity of the data controller, (ii) the purpose of data processing and (iii) the categories of data recipients if the data shall be disclosed to third parties. Further, in relation to the processing of sensitive personal data implied consent is not sufficient; consent must be given expressly.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

55. TAIWAN

CONTRIBUTION DETAILS

Formosa Transnational Attorneys at Law
www.taiwanlaw.com

Chun-yih Cheng
Senior Partner
T +886 2 27557366 Ext 158
chun-yih.cheng@taiwanlaw.com

LAW

The former Computer Processed Personal Data Protection Law ("**CPPL**") was renamed as the Personal Data Protection Law ("**PDPL**") and amended on 26 May 2010. The PDPL became effective on 1 October 2012, except that the provisions relating to sensitive personal data and the notification obligation for personal data indirectly collected before the effectiveness of the PDPL remain ineffective. The government has proposed further amendment to these provisions, which is pending legislative review. The information hereunder is based upon the effective PDPL only.

DEFINITION OF PERSONAL DATA

According to PDPL, personal data means the name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and other information which may directly or indirectly be used to identify a living natural person.

DEFINITION OF SENSITIVE PERSONAL DATA

According to PDPL, sensitive personal data means the personal data relating to medical treatments, genetic information, sex life, health checks and criminal records. As mentioned above, the provisions relating to sensitive personal data remain ineffective. At the moment, sensitive personal data will be treated like other data.

NATIONAL DATA PROTECTION AUTHORITY

In Taiwan, there is no single national data protection authority. The various ministries and city/county governments serve as the competent authorities.

REGISTRATION

Unlike the CPPL, there is no need to register with any authorities for the collection, processing, usage and international transfer of personal data under the PDPL.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DATA PROTECTION OFFICERS

There is no requirement in Taiwan for the data controller to appoint a data protection officer. However, if the data controller is a government agency, a specific person should be appointed to be in charge of the security maintenance measures.

COLLECTION AND PROCESSING

Under the PDPL, the data controller should not collect or process personal data unless there is specific purpose and should comply with one of the following conditions:

- where collection/processing is explicitly stipulated by law;
- where there is a contract or quasi contract between the data controller and the data subject;
- where the data subject has his/herself disclosed such data or where the data has been publicised legally;
- where it is necessary for public interest on statistics or the purpose of academic research conducted by a research institution. The data may not lead to the identification of a certain person after the treatment of the provider or by the disclosure of the collector;
- where written consent has been given by the data subject;
- where the public interest is involved; or
- where the personal data is obtained from publicly available sources, except that where the is vital interest of the data subject requires more protection and the prohibition of the processing or usage of such personal information.

Furthermore, except for the exemptions stipulated in the PDPL (e.g. if it is explicitly stipulated by law that the provision of such information is not required), the data controller is permitted to collect and process personal data only if the data controller unambiguously informs the data subject of the following information prior to or upon the collection:

- data controller's name;
- purpose for collecting personal data;
- categories of personal data;
- period, area, recipients and means of using the data;
- the data subject's rights and the methods by which the data subject may exercise those rights in accordance with the PDPL; and
- that the data subject has the right to choose whether or not to provide the data and the consequences of not providing the data.

The information collected should in principle only be used for the purpose notified and not for any other purpose.

TRANSFER

The central competent authority may restrict the international transfer of personal data by the data controller which is not a government agency if:

- it involves major national interests;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- where a national treaty or agreement specifies otherwise;
- where the country receiving personal data lacks proper regulations that protect personal data and that might harm the rights and interests of the data subject;
- where the international transfer of personal data is made to a third country through an indirect method in order to evade the provisions of the PDPL.

SECURITY

Data controllers which are non government agencies should adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed.

The central competent authority may request the data controller to set up a plan for the security measures of the personal data file or the disposal measures for the personal data after termination of business.

BREACH NOTIFICATION

Where the personal data is stolen, disclosed, altered or infringed in other ways due to the violation of the PDPL, the data controller should notify the data subject.

ENFORCEMENT

Under the PDPL, the competent authority may perform an inspection, if it is necessary for the protection of personal data, of the disposal measures after termination of business, the limitation of international transfer, other routine examinations, or if the PDPL may be violated. Those who perform the inspection may ask the data controller to provide a necessary explanation, take cooperative measures, or provide relevant evidence.

When the competent authority conducts such an inspection, it may seize or duplicate the personal data and files may be confiscated or may be used as evidence. The owner, holder or keeper of that data or those files should surrender them upon request.

In addition, a breach of the PDPL may be subject to criminal sanctions, administrative fines, and civil compensation (class action is permitted).

ELECTRONIC MARKETING

The PDPL applies to electronic marketing in the same way as to other marketing. Within the necessary scope of specific purposes of data collection, the data controller may use personal data for marketing. However, when the data subject refuses the marketing (a right to "opt-out"), the data controller should cease using such personal data for marketing. In addition, when making the first marketing, the data controller should bear the costs to provide the data subject with the means to refuse marketing.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no special law or regulation applicable to online privacy. The PDPL applies to online and physical world in the same manner. As a result, online unique issues are not specifically addressed.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

56. THAILAND

CONTRIBUTION DETAILS

Dr. Chanvitaya Suvarnapunya
Partner
T +662 686 8500
chanvitaya.suvarnapunya@dlapiper.com

Chadaporn Ruangtoowagoon
Senior Associate
T +662 686 8579
chadaporn.ruangtoowagoon@dlapiper.com

LAW

At present, Thailand does not have any general statutory law governing data protection or privacy. However, the Constitution of the Kingdom of Thailand does recognize the protection of privacy rights. In addition, statutory laws in some specific areas (such as telecommunications, banking and financial businesses ("**Specific Businesses**") as well as other non-business related laws, such as certain provisions under Thai Penal Code and the Child Protection Act B.E. 2543 (2003), do provide a certain level of protection against any unauthorised collection, processing, disclosure and transfer of personal data.

Recently, the draft Personal Information Protection Act ("**Draft**"), which has been reviewed by the Council of State, was given to the Committee for House of Representative Coordination to review and analyse if there are any practical issues on applying the law and how the Data Protection Committee should be formed.

The Draft is being reviewed by the Office of the Public Sector Development Commission and will be submitted to the Cabinet for approval later. The current Draft provides protection of personal data by restricting the gathering, using, disclosing and altering of any personal data without the consent of the data owner. The Draft also imposes both criminal penalties and civil liability for any violation of the Draft and calls for the establishment of a Protection of Personal Data Commission to regulate compliance with the Draft.

Notwithstanding the above, at present, no clear indication exists as to when the Draft will be final, or whether it will ultimately be enacted into binding law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF PERSONAL DATA

According to the Draft, "personal data" means any information or data relating to an identified natural person or that can identify a natural person by reference to the facts, data or any other materials about that natural person.

The information or data may be in the form of documents, files, reports, books, charts, portraits, photos, films, recorded images or sounds that may be kept or stored in computer machines or in any other means that can be used to make the recorded information or data seen. Personal Data shall also include facts about, or behaviours of, a deceased person.

DEFINITION OF SENSITIVE PERSONAL DATA

Not available in the present Draft.

NATIONAL DATA PROTECTION AUTHORITY

None at present – see detail in "Law" section above.

REGISTRATION

No registration requirement with respect to the collection or use of personal data exists.

DATA PROTECTION OFFICERS

No requirement exists in Thailand for an organisation to appoint a data protection officer.

COLLECTION AND PROCESSING

Statutory laws provide a certain level of protection for the accumulation, retention and release of personal data for Specific Businesses.

For example, a telecommunications operator may collect personal data from customers only for the purpose of its business operation and as permissible by law. The collection of sensitive information, such as physical handicaps or genetics, is strictly prohibited. Operators must also have proper security measures in place to protect customers' data, including any of their personal data. Any release of personal data, except disclosure for national security purposes, requires the data owner's consent.

According to the Child Protection Act, the guardian of a child's safety or a child's safety protector are forbidden to disclose the name, surname, picture or any information regarding the child and the child's guardian in a manner which is likely to be detrimental to the reputation, esteem or entitlements of the child. This is also applied *mutatis mutandis* to a competent official, social worker, psychologist or person having the duty to protect a child's safety, who has come into the possession of such information as a result of the performance of his or her duties. It is also forbidden for any person to advertise or disseminate by means of the mass media or any other form of information technology the disclosed information in violation of the aforementioned provisions.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

If no specific statutory law is applicable then generally, the collection and processing of personal data with the consent (preferably written) of the data owner is permissible.

TRANSFER

Under the Thai Civil and Commercial Code, a person who wilfully, negligently, or unlawfully injures the life, body, health, liberty, property or any right of another person has committed a wrongful act and is required to compensate the victim. Disclosure or transfer of data may be considered a wrongful act if it causes damage to the data owner.

In practice, the prior written consent of the data owner should be obtained before transferring the data to any third person. Disclosure of data without the consent of the data owner is permissible in very limited circumstances (e.g. pursuant to an order from a government authority or Thai court).

SECURITY

Data controllers in Specific Businesses are required to maintain an appropriate level of security to protect any stored personal data from unauthorised access. Failure to comply with this requirement normally results in both imprisonment and monetary penalties.

Data controllers in non-Specific Businesses are also recommended to implement appropriate security measures to protect personal data from unauthorised access. If unauthorised access causes any damage to the data owner, the data controller may also be liable under the Thai Civil and Commercial Code for committing a wrongful act by failing to prevent the unauthorised access.

BREACH NOTIFICATION

No notification requirement exists with respect to privacy or data protection law.

ENFORCEMENT

No organisation in Thailand is primarily responsible for the enforcement of privacy or data protection law.

ELECTRONIC MARKETING

Presently, there is no specific law that prohibits the use of personal data for the purposes of electronic marketing. The availability of option for opt-in and opt-out is just the practice as a norm and not yet the law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

At present, there is no provision under the relevant laws and the Draft that specifically prohibits or controls the placing of cookies on users' computers.

Although there are provisions under the Computer Crime Act B.E. 2550 (2007), imposing punishments for certain computer data alterations, the computer cookies or location tracing mechanisms are excluded as they will not cause any of the above alterations to happen to computers. Those below acts are punishable:

- Any person who illegally damages, destroys, corrects, changes or amends a third party's computer data, either in whole or in part, shall be subject to imprisonment for no longer than 5 years or a fine of not more than THB 100,000, or both.
- Any person who illegally commits any act that causes the working of a third party's computer system to be suspended, delayed, hindered or disrupted to the extent that the computer system fails to operate normally shall be subject to imprisonment for no longer than 5 years or a fine of not more than THB 100,000, or both.
- Any person sending computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person's normal operation of their computer system shall be subject to a fine of not more than THB 100,000.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

57. TRINIDAD AND TOBAGO

CONTRIBUTION DETAILS

M. Hamel Smith & Co.
11 Albion Street
Corner Dere and Albion Street
Port of Spain
www.trinidadlaw.com
T +1 868 821 5500
F +1 868 625 9177

Jonathan Walker
Partner
T +1 868 821 5500 ext. 5625
jonathan@trinidadlaw.com

Aisha Peters
Associate
T +1 868 821 5500 ext. 5603
aisha@trinidadlaw.com

LAW

In Trinidad and Tobago *The Data Protection Act, 2011* provides for the protection of personal privacy and information ("**DPA**") processed and collected by public bodies and private organisations.

The DPA was partially proclaimed on the 6th January 2012 by Legal Notice 2 of 2012 and only Part I and sections 7 to 18, 22, 23, 25(1), 26 and 28 of Part II have come into operation.

No timetable has been set for the proclamation of the remainder of the DPA and it is possible that there may be changes to the remainder of the legislation before it is proclaimed.

DEFINITION OF PERSONAL DATA

Personal Data (which is referred to in the DPA as "Personal Information") is defined as information about an identifiable individual that is recorded in any form including:

- the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;
- the address and telephone number of the individual;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- any identifying number, symbol or other particular identifier designed to identify the individual;
- information relating to the individual's race, nationality or ethnic origin, religion, age or marital status;
- information relating to the education or the medical, criminal or employment history of the individual or information relating to the financial transactions in which the individual has been involved or which refer to the individual;
- correspondence sent to an establishment by the individual;
- information that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence that would reveal the contents of the original correspondence;
- the views and opinions of any other person about the individual; or
- the fingerprints, DNA, blood type or other biometric characteristics of the individual.

DEFINITION OF SENSITIVE PERSONAL DATA

Sensitive Personal Data (which is referred to in the DPA as "sensitive personal information") is defined as personal information on a person's:

- racial or ethnic origins:
- political affiliations or trade union membership;
- religious beliefs or other beliefs of a similar nature;
- physical or mental health or condition;
- sexual orientation or sexual life; or
- criminal or financial record.

NATIONAL DATA PROTECTION AUTHORITY

The entity responsible for the oversight, interpretation and enforcement of the DPA is the Office of the Information Commissioner. It has broad authority, including to authorise the collection of personal information about an individual from third parties and to publish guidelines regarding compliance with the Act.

REGISTRATION

There is no registration requirement under the DPA.

DATA PROTECTION OFFICERS

There is no requirement for organisations to appoint a data protection officer.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

COLLECTION AND PROCESSING

The knowledge and consent of the individual is required for the collection, use and disclosure of personal information. Furthermore, collection is required to be undertaken in accordance with the purpose identified by the organisation doing the collecting and other legal requirements.

Sensitive personal information may not be processed except as specifically permitted by law.

The DPA includes provisions that relate specifically to the collection and processing of personal information by public bodies and private enterprises respectively, however these are not yet in force. Nevertheless, they are presented below.

Public Bodies

Part III of the DPA provides that a public body may collect and process personal data when the following conditions are met:

- the collection of that information is expressly authorised by law;
- the information is collected for the purpose of law enforcement;
- the information relates directly to and is necessary for an operating programme or activity of the public body;
- the collection of personal information is collected directly from the individual unless (a) another method of collection is authorised by the individual, Information Commissioner or law; (b) the information is necessary for medical treatment; (c) the information is required for determining the suitability of an award; (d) for judicial proceedings; (e) the information is required for the collection of a debt or fine; (f) it is required for law enforcement;
- the individual is informed of the purpose for collecting his/her personal information; the legal authorisation for collecting it and contact details of the official or employee of the public body who can answer the individuals questions about the collection.

Private Bodies

Part IV of the DPA provides that the collection and processing of personal information by private organizations will be in accordance with certain Codes of Conduct (which are to be determined by the Office of the Information Commissioner in consultation with the private sector) and with the General Privacy Principles (which are currently in force).

Sensitive Information

As to both public bodies and private organizations, Sensitive Personal Information may not be processed without the consent of the individual unless (i) it is necessary for the healthcare of the individual; (ii) the individual has made the information public; (iii) it is for research or statistical analysis; (iv) it is by law enforcement; (v) for the purpose of determining access to social services; or (vi) as otherwise authorised by law.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

Section 6(1) of the DPA provides that personal information may be transferred outside of Trinidad and Tobago only if the foreign country requesting the individual's personal information has safeguards for the regulation of the personal information which are comparable to Trinidad and Tobago's.

In this regard, the Office of the Information Commissioner is required to publish in the *Gazette* and at least two newspapers in daily circulation in Trinidad and Tobago a list of countries which have comparable safeguards for personal information as provided by this Act. As of February 1, 2013, this has not yet happened because a Commissioner has yet to be appointed.

Sections 72(1) and (2) of the DPA (neither of which are in force as yet) provide that where a mandatory code is developed for private bodies it must require at a minimum that personal information under the custody or control of a private organization not be disclosed to a third party without the consent of the individual to whom it relates, subject to certain conditions. Where personal information under the custody and control of an organization is to be disclosed to a party residing in another jurisdiction, the organization must inform the individual to whom the information relates.

Section 6 of the DPA, which is in force, states that all persons who handle, store or process personal information belonging to another person are subject to the following "General Privacy Principles";

- an organization shall be responsible for the personal information under its control;
- the purpose for which personal information is collected shall be identified by the organization before or at the time of collection;
- knowledge and consent of the individual are required for the collection, use or disclosure of personal information;
- collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization;
- personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual;
- personal information shall be accurate, complete and up-to-date, as is necessary for the purpose of collection;
- personal information is to be protected by such appropriate safeguards having regard to the sensitivity of the information;
- sensitive personal information is protected from processing except where specifically permitted by written law;
- organizations are to make available to individuals documents regarding their policies and practices related to the management of personal information, except where otherwise provided by written law;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- 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, such that the individual can challenge the accuracy and completeness of the information;
- the individual has the ability to challenge the organization's compliance with the above principles and receive timely and appropriate engagement from the organization; and
- personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

SECURITY

The DPA generally requires that personal information be protected by appropriate safeguards based on the sensitivity of the information. Sensitive personal information may not be processed except where permitted by law.

BREACH NOTIFICATION

There is no provision in the DPA for notifying data subjects or the Information Commissioner of a security breach.

ENFORCEMENT

The Office of the Information Commissioner is responsible for monitoring the administration of this Act to ensure that its purposes are achieved (s.9 (1)).

The Information Commissioner has several broad powers to conduct audits and investigations of compliance with the DPA.

Part V of the DPA (which is not in force) details the penalties for contraventions of the DPA and also makes further provisions for the enforcement of the DPA.

ELECTRONIC MARKETING

The DPA has no specific provision regarding electronic marketing.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The DPA has no specific provision regarding online privacy.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

58. TURKEY

CONTRIBUTION DETAILS

Burak Özdağıstanli
Associate
T +90 212 318 05 16
bozdagistanli@yukselkarkinkucuk.av.tr

İrem Cansu Atikcan
Associate
T +90 212 340 05 96
iatikcan@yukselkarkinkucuk.av.tr

LAW

Currently, there is no specific law in Turkey regarding personal data protection. Data protection is governed by the general provisions of a number of laws and regulations.

There has been a Draft Law on the Protection of Individuals with regard to Processing of Personal Data ("**Draft Law**") pending before the Turkish Parliament, which is reformulated over the last months of 2012. The Draft Law regulates rules and procedures relating to protection and processing of personal data and has been prepared in light of European Union Directive 95/46/EC and the Commission's Decision 2001/497/EC.

On 12 September 2010, a referendum was held on a reform package which introduced amendments to the last Turkish Republic Constitution adopted in 1980. As a result of the amendment, the right to protection of personal rights and privacy set forth in Article 20 of the Constitution has been bolstered, increasing the scope of accountability and introducing more stringent requirements for protection of personal data. It is anticipated that the Draft Law shall be enacted in the very near future to reflect changes made to the Turkish Constitution.

Most recently on 24 July 2012 Regulation on Protection of Personal Data in Electronic Communications Sector was published. This Regulation stipulates sector specific requirements for operators.

DEFINITION OF PERSONAL DATA

In the absence of a specific law on data protection there is no exact definition for "personal data" however there are some regulations and laws that have defined personal data within their specific context.

The most relevant source is the Regulation on Protection of Personal Data in Electronic Communications Sector which deals with personal data processed in hard copy and automated fashion, this Regulation defines personal data as any information regarding a known or identifiable natural or legal person.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF SENSITIVE PERSONAL DATA

Although there is no explicit definition of sensitive data, the Turkish Criminal Code No. 5237 imposes penalties on any person who records the political, philosophical or religious concepts of individuals, or without legitimate reason personal information relating to their racial origins, ethical tendencies, health conditions or connections with syndicates.

DEFINITION OF PERSONAL DATA

The Draft Law defines personal data as any information relating to an identified or identifiable natural and legal person.

DEFINITION OF SENSITIVE PERSONAL DATA

The Draft Law defines sensitive personal data as personal data revealing race, political opinions, philosophical beliefs, religion, sect or other beliefs, foundation or union membership, and the processing of data concerning health or private life and all kinds of convictions.

NATIONAL DATA PROTECTION AUTHORITY

Currently there is no independent body governing data protection in Turkey.

In accordance with the Draft Law an independent authority will be established to monitor data processing and ensure compliance, namely, the Personal Data Authority ("**Authority**"). The Authority shall enforce application of the law, monitor data processing and ensure compliance.

REGISTRATION

Currently there is no requirement for registration.

The Draft Law stipulates that the Authority shall keep a Personal Data Registry, natural and legal persons will be required to register prior to commencing any data processing activities unless an exemption applies.

DATA PROTECTION OFFICERS

There is no requirement in Turkey to appoint a data protection officer.

Neither, under the Draft Law is there any requirement to appoint a data protection officer.

COLLECTION AND PROCESSING

Article 20 of the Constitution states that everyone has the right to ask for protection of his/her personal information; and such right includes the right to be informed of personal data pertaining to such person, the right to access, delete and/or correct such data and the right to find out whether the data is being used in accordance with the purpose for which it was collected.

The provision also stipulates that personal data can only be processed for reasons stated in the law or with explicit consent of the data subject.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Data protection is enforced through general provisions laid down in a number of laws and regulations. In this regard, each situation needs to be evaluated individually as it may be subject to provisions of an applicable specific law, if any.

In general terms, the Turkish Criminal Code No. 5237 contains provisions regulating collecting and processing of personal data and imposes penalties for acquiring and unlawful recording of personal data.

Furthermore, the Turkish Criminal Code No. 5237 stipulates that upon expiry of the time period specified by law to retain data, such data must be deleted or destroyed.

The Draft Law stipulates personal data can only be processed in accordance with the Draft Law and other laws and sets forth personal data may be collected and processed if:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed;
- accurate and, where necessary, kept up to date; or
- 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 or for which they are further processed.

Personal data may be processed only if:

- the data subject has given his explicit consent;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the life or physical integrity of the data subject or another where the data subject is incapable of giving his consent;
- processing is necessary for the execution or performance of a contract to which the data subject is party;
- processing of data that has been disclosed/published by the data subject or is available in the public domain; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

- the identity of the controller and of his representative, if any;
- the purposes of the processing for which the data is intended;
- the recipients of the data;
- the process of collecting data, the legal grounds and probable effects;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- the existence of the right of access data collected; and
- the right to rectify the data concerning the data subject.

Where the data has not been obtained from the data subject, the controller shall provide the data subject with the above stated information as well as details of the categories of data concerned.

Processing of sensitive personal data revealing race, political opinions, philosophical beliefs, religion, sect or other beliefs, foundation or union membership, and the processing of data concerning health or private life and all kinds of convictions is forbidden.

Sensitive personal data may be processed under a number of circumstances defined under the Draft Law provided precautions/safeguards are taken to protect the family and private life.

TRANSFER

Broadly speaking, the Turkish Criminal Code No. 5237, contains provisions regarding unlawful transmission or obtaining of personal data. Nonetheless, each situation should be evaluated as it may be subject to provisions of an applicable specific law.

In accordance with the Draft Law approval of the Authority is required for transfer of personal data and personal data may only be transferred to a third country if; the recipient country ensures an adequate level of protection, if there is no such protection in the recipient foreign country, the data transfer may be permitted in a number of situations listed under the Draft Law.

SECURITY

Consistent with the principles of good faith those entrusted with personal data are expected to ensure protection of such data. There are a number of specific laws which require data to be kept safely and ensure protection of any data collected and/or processed.

Under the Draft Law, the controller is required to ensure that appropriate technical and organisational measures are taken to prevent all illegal processing and to ensure the data is not destroyed, lost, amended, disclosed or transferred without authority. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.

In the event the controller carries out processing by way of a processor, such relationship must be governed by a contract or legal act binding the processor to the controller and such instrument shall stipulate that the processer has adequate technological and administrative precautionary measures in place.

BREACH NOTIFICATION

There is no breach notification requirement; nonetheless, in the event that data is inadvertently or erroneous lost, transferred, destroyed etc., notification should be made to the data subjects in accordance with the principles of good faith. Furthermore, each situation should be evaluated in accordance with provisions of the applicable specific law, if any, as more strict procedures may apply.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The Draft Law does not currently stipulate any breach notification requirement; however, this may change before the law is enacted.

ENFORCEMENT

In general terms, the Turkish Criminal Code No. 5237 imposes custodial sentences for unlawful processing of data; the Turkish Civil Law No. 4721 affords the right to claim compensation for the unjust use of data and a number of other laws impose administrative fines.

The Draft Law also introduces imprisonment, penalties and administrative fines for collecting and processing personal data in breach of the law and disclosing it illegally to third parties. Acts that breach the Draft Law can result in administrative fines in the amount of 5,000 TL (approximately EUR 2,500) to 10,000 TL (approximately EUR 5,000) to be imposed by the Authority.

ELECTRONIC MARKETING

There is another Draft Law on E-Commerce pending before the Parliament which would require service providers to provide protection for personal data.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no specific law on online privacy with specific provisions on Cookies and Location Data. However, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting enables internet users to initiate prosecution in case of infringements of their personal rights.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

59. UAE

CONTRIBUTION DETAILS

Paul Allen
Head of Intellectual Property & Technology – Middle East
T +971 4 438 6295
paul.allen@dlapiper.com

Ken Dearsley
Senior Counsel
T +971 4 438 6286
ken.dearsley@dlapiper.com

Jamie Ryder
Legal Consultant
T +971 4 438 6297
jamie.ryder@dlapiper.com

Robert Flaws
Legal Consultant
T +971 4 438 6287
robert.flaws@dlapiper.com

DATA PROTECTION OFFICERS

There is no requirement in the UAE for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

If the collection and processing of any personal data pertains to an individual's private or family life then the consent of the individual is required. A failure to obtain such consent would constitute a breach of the Penal Code (Article 378) and could also be a breach of the:

- Cyber Crime Law if the personal data is obtained or processed through the internet or electronic devices in general (Articles 21 and 22); and
- Telecoms Law to the extent that data is obtained through any means of telecommunication, including through a telecommunications service provider, or any other electronic means (Clause 3 Privacy of Consumer Information Policy).

Additionally, unlawful access via the internet of electronic devices of financial information (e.g. Credit Cards and Bank Accounts) without permission is an offence under the Cyber Crime Law (Articles 12 and 13).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

TRANSFER

According to the Penal Code (Clause 379), personal data may be transferred to third parties inside and/or outside of the UAE if the data subjects have consented in writing to such transfer.

The requirement to obtain the written consent may be waived, pursuant to the Penal Code (Article 377) and Clause 3 of the Privacy of Consumer Information Policy, where:

- a UAE official/public authority has required the transfer of such data to it; and
- the transfer serves public interests or national security.

SECURITY

There are no specific provisions under UAE Federal Law relating to the type of measures to be taken or level of security to have in place against the unauthorised disclosure of personal data. Instead, the Cyber Crime Law focuses on offences related to accessing data without permission and/or illegally (Articles 2 and 3 of the Cyber Crime Law), including financial information (e.g. credit card information or bank account information) (Articles 12 and 13).

The Policies require telecommunications service providers to "take measures to prevent the unauthorised use or disclosure of consumer information", "strive to protect the privacy of consumer personal data that they maintain in their files whether in electronic or paper form" and "limit access to consumer information to trained and authorised staff" (Clause 3 of the Privacy of Consumer Information Policy).

Based on the above, best practice from a UAE law perspective would be to take appropriate technical security measures against unauthorised or unlawful processing of, and against accidental disclosure of, personal data. The measures taken must ensure a level of security adequate enough to minimise the risk of liability arising out of a claim for breach of privacy made by a data subject.

BREACH NOTIFICATION

In principle, there is no mandatory requirement under UAE Federal Law to report data security breaches.

Data subjects based in the UAE, however, may be entitled to hold the entities in possession of their data, liable under the principles of the UAE Civil Code for their negligence in taking proper security measures to prevent the breach, if such breach has resulted in actual losses being suffered by the data subjects.

In relation to telecommunication services, the Telecoms Law and most Policies do not include an explicit requirement on service providers to take the initiative in notifying the TRA of a breach or alleged breach, unless a subscriber complains to a service provider about the unauthorised disclosure of his or her personal data (Clause 3.2.2 of the Consumer Complaint and Dispute Resolution Policy).

Subscribers are also able to complain direct to the TRA about the unauthorised disclosure of their personal data (Clause 3.3 of the Consumer Complaint and Dispute Resolution Procedures and Clause 4.1 of the Consumer Complaint and Dispute Resolution Policy).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ENFORCEMENT

There are three possible methods of enforcement from a UAE law perspective:

1. Where the unauthorised disclosure of personal data results in a breach of the Penal Code:

The Public Prosecutor in either the Emirate:

- where the party suspected of the breach ("**Offender**") resides; or
- where the disclosure occurred

will have jurisdiction over a data subject's complaint.

If after concluding investigations with the police, the Public Prosecutor is satisfied with the evidence compiled, charges may be brought against the suspect.

The case would then be transferred to the Criminal Courts of First Instance. The data subject may attach a civil claim to the criminal proceedings before the Courts have ruled on the case.

Pursuant to the Penal Code (Article 379), if the Courts find a suspect guilty of disclosing secrets that were entrusted to him "by reason of his profession, craft, situation or art" the penalties to be imposed under the Penal Code may include a fine of up to UAE Dirhams 20,000 (the fine is determined by the Courts) and an imprisonment for at least one year (Article 379). More generally, pursuant to the Penal Code (Article 378), "a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals' private or family life" by committing any of the acts described under Article 378 "other than the legally permitted cases or without the victim's consent."

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the data subject to the Civil Courts of First Instance for further consideration. The data subject would need to prove the losses he/she has suffered as a direct result of the disclosure of his/her personal data before the Civil Courts in order for damages to be awarded.

2. Where the unauthorised disclosure of personal data results in a breach of the Cyber Crime Law:

The police in each Emirate have developed specialised cybercrime units to handle complaints that relate to breaches of the Cyber Crime Law.

As above, the cybercrime unit in the Emirate where:

- the Offender resides; or
- where the disclosure occurred

will have jurisdiction over a data subject's complaint.

The cybercrime unit would investigate the case and decide whether or not to refer it to the Public Prosecutor in the same Emirate. If the case is referred and the Public Prosecutor is satisfied with the findings of the cybercrime unit, charges would be brought against the suspect. The same procedure identified above is then followed before the Courts.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

If found guilty of an offence under the Cyber Crime Law, the punishment an Offender can receive under the Cyber Crime Law varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and/or a fine between AED 150,000 and 1,000,000 (Articles 2, 3, 7, 21 and 22 of the Cyber Crime Law). If found guilty of an attempt to commit any of the relevant offences under the Cyber Crime Law, the punishment is half the penalty prescribed for the full crime (Article 40).

3. Where the unauthorised disclosure of personal data results in a breach of the Telecoms Law and Policies:

The TRA is responsible for overseeing the enforcement of the Telecoms Law and in this regard may rely on the Police and Public Prosecutor in the Emirate where, either;

- the breach has occurred; or
- where the suspect resides.

Where a licensed telecommunications service provider has breached the law, the subscriber/data subject generally needs to complain first to the service provider about the breach (Clause 3.1 Consumer Complaint and Dispute Procedure), though a direct approach to the TRA may be possible (Clause 4.1 of the Consumer Complaint and Dispute Resolution Policy). The subscriber may complain to the TRA if the breach is not satisfactorily resolved within:

- thirty days as of the date of the complaint (Clause 2.2.1 Consumer Complaint and Dispute Procedure); or
- a longer period if the service provider notifies the subscriber of this extended period (Clause 2.2.1 Consumer Complaint and Dispute Procedure).

The subscriber's complaint needs to be submitted to the TRA within three months of the date when the service provider last took action (Clause 3.2 Consumer Complaint and Dispute Procedure). This three months requirement may be waived subject to the discretion of the TRA (Clause 3.3 Consumer Complaint and Dispute Procedure).

After examining the complaint the TRA may direct the service provider "to undertake any remedy deemed appropriate" to the subscriber/data subject (Clause 4.3 Consumer Complaint and Dispute Policy).

ELECTRONIC MARKETING

No express laws are outlined under UAE law covering electronic marketing. However, Articles 21 and 22 of the Cyber Crime Law and Clause 3 of the Privacy of Consumer Information Policy, as described in the 'Collection and Processing' section above, are worded widely enough to potentially apply to electronic marketing. Article 22 of the Cyber Crime Law, for example, prohibits the use of various electronic devices in order to disclose, without permission, confidential information that has been obtained through the course of a person's duties.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Although the UAE Penal Code does not contain provisions directly relating to the internet, its provisions related privacy are broadly drafted and therefore could apply to online matters (such as Article 378 as described above).

Additionally, as described in the 'Collection and Processing' section above, under certain circumstances, online privacy is protected through Articles 21 and 22 of the Cyber Crime Law and Clause 3 of the Privacy of Consumer Information Policy. Unlawful access via the internet, by electronic devices, of financial information (e.g. Credit Cards and Bank Accounts) without permission is also an offence under the Cyber Crime Law (Articles 12 and 13).

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

60. UK

CONTRIBUTION DETAILS

Cameron Craig
Partner & Co-Chair of EMEA Data Protection and Data Privacy Group
T +44 (0)207 796 6574
M +44 (0)7971 142 352
cameron.craig@dlapiper.com

Paul McCormack
Solicitor
T +44 (0)207796 6140
M +44 (0)7968 558852
paul.mccormack@dlapiper.com

LAW

As a member of the European Union, the United Kingdom implemented the EU Data Protection Directive 95/46/EC in March 2000 with the Data Protection Act 1998 ("**Act**"). Enforcement is through the Information Commissioner's Office ("**ICO**").

DEFINITION OF PERSONAL DATA

"Personal data" is defined under the Act as data relating to living individuals who can be identified a) from the data, or b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

DEFINITION OF SENSITIVE PERSONAL DATA

"Sensitive personal data" means personal data consisting of information as to: (a) the racial or ethnic origin of the data subject; (b) his political opinions; (c) his religious beliefs or other beliefs of a similar nature; (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); (e) his physical or mental health or condition; (f) his sexual life; (g) the commission or alleged commission by him of any offence; or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
T +0303 123 1113 (or +44 1625 545745 if calling from overseas)
F 01625 524510
www.ico.gov.uk

REGISTRATION

Data controllers who process personal data must inform the Information Commissioner so that their processing of personal data may be registered and made public in the Register of data controllers, unless an exemption applies. Any changes to the processing of personal data will require the registration to be amended.

The notification should include the following information:

- what data is being collected;
- why the data will be processed;
- the categories of data subject; and
- whether the data will be transferred either within or outside the European Economic Area.

DATA PROTECTION OFFICERS

There is no requirement in the UK for organisations to appoint a data protection officer.

COLLECTION AND PROCESSING

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

- the data subject consents;
- the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party;
- the processing satisfies the data controller's legal obligation;
- the processing protects the data controller's vital interests;
- the processing is required by an enactment, the Crown or the government;
- the processing is required to perform a public function in the public interest, or to administer justice; or
- the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions.

Whichever of the above conditions is relied upon, the data controller must provide the data subject with "fair processing information". This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.

TRANSFER

Data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met:

- the data subject consents;
- the transfer is essential to a contract to which the data subject is party;
- the transfer is needed to carry out a contract between the data controller and a third party if the contract serves the data subject's interests;
- the transfer is legally required or essential to an important public interest;
- the transfer protects the data subject's vital interests; or
- the data is public.

Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides "adequate protection" for the security of the data, or if the transfer is covered by "standard contractual clauses" approved by the European Commission, or subject to an organisation's Binding Corporate Rules. There is no requirement in the UK to notify the ICO of the use of the standard contractual clauses or to file these with the ICO.

For transfer of data to the United States, compliance with the US/EU Safe Harbor principles can satisfy the requirements of the UK's transfer restrictions.

SECURITY

Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data.

The Act does not specify specific security measures to adopt and implement. However, the ICO recommends that organisations should adopt best practice methodologies such as ISO 27001.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

BREACH NOTIFICATION

There is no mandatory requirement in the Act to report data security breaches or losses to the ICO or to data subjects, however, ICO guidance indicates that if a large number of people are affected or the consequences of the breach are particularly serious, the ICO should be informed.

Sector specific regulations/guidance also imposes obligations to notify the relevant regulation and data subjects in the event of a security breach (e.g. the Financial Services Authority).

MANDATORY BREACH NOTIFICATION

None contained in the Act. However, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PEC Regulations"), as amended, require providers of a public electronic communications service ("service providers") to notify the ICO (and in some cases subscribers) in the event of a personal data breach.

Failure to notify can result in a fine of GBP 1,000 and negative publicity.

ENFORCEMENT

In the UK the Information Commissioner is responsible for the enforcement of the Act. If the Information Commissioner becomes aware that a data controller is in breach of the Act, he can serve an enforcement notice requiring the data controller to rectify the position. Failure to comply with an enforcement notice is a criminal offence and can be punished with fines of up to GBP 5,000 in the Magistrates' Court or with unlimited fines in the Crown Court.

Additionally, the Information Commissioner can impose fines of up to GBP 500,000 for serious breaches of the Act. This penalty, introduced in April 2010, can be imposed in respect of breaches of the data protection principles which are:

- serious; and
- likely to cause substantial damage or distress; and either
- the contravention was deliberate; or
- the data controller knew or ought to have known that there was a risk that the breach would occur and would be likely to cause substantial damage or distress, but failed to take reasonable steps to prevent the breach.

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (e.g. an email address is likely to be "personal data" for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (e.g. a right to "opt-out") for direct marketing purposes.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

There are a number of different opt-out schemes/preference registers for different media types. Individuals (and, in some cases, corporate subscribers) can contact the following schemes and ask to be registered as not wishing to receive direct marketing material. If advertising materials are sent to a person on the list, sanctions can be levied by the ICO using his powers under the Act.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient and unsolicited emails can only be sent without consent if:

- The contact details have been provided in the course of a sale;
- The marketing relates to a similar product; and
- The recipient was given a means of refusing the use of their contact details for marketing when they were collected.

Direct marketing emails must not disguise or conceal the identity of the sender. SMS marketing is also likely to be included within the prohibition on email marketing.

The restrictions on marketing by email only applies in relation to individuals and not where email marketing is sent to corporations.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

The PEC Regulations (as amended by Directive 2009/12/EC) deals with the collection of location and traffic data by public electronic communications services providers ("**CSPs**") and use of cookies (and similar technologies).

Traffic Data – Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if:

- It is being used to provide a value added service; and
- Consent has been given for the retention of the Traffic Data.

Traffic Data can only be processed by a CSP for:

- The management of billing or traffic;
- Dealing with customer enquiries;
- The prevention of fraud; or
- The provision of a value added service.

Location Data – Location Data may only be processed for the provision of value added service with consent.

CSPs are also required to take measures and put a policy in place to ensure the security of the personal data they process.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Cookie Compliance – The use and storage of cookies and similar technologies requires: a) clear and comprehensive information; and b) consent of the website user. The ICO has confirmed that implied consent will also be a valid form of consent under certain circumstances. The PEC Regulations allow for the continued use of the website to be taken as an indication of implicit consent, subject to the requirement to provide relevant information.

Consent is not required for cookies that are;

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

Enforcement of a breach of the PEC Regulations is dealt with by the ICO and sanctions for breach are the same as set out in the Enforcement section above.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

61. UKRAINE

CONTRIBUTION DETAILS

Natalia Pakhomovska
Legal Director
T +380 44 495 1789
natalia.pakhomovska@dlapiper.com

Roman Inozemtsev
Associate
T +380 44 490 9575
roman.inozemtsev@dlapiper.com

Natalia Kirichenko
Associate
T +380 44 490 9575
natalia.kirichenko@dlapiper.com

LAW

The Law of Ukraine No. 2297 VI "On Personal Data Protection" as of 1 June 2010 ("**Data Protection Law**") is the main legislative act regulating relations in the sphere of personal data protection in Ukraine. At 20 December 2012 Data Protection Law has been substantially amended by the Law of Ukraine "On introducing amendments to the Law of Ukraine On Personal Data Protection" dated 20 November 2012 No. 5491-VI ("**Amendments to the Data Protection Law**").

In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law.

The Data Protection Law essentially complies with EU Data Protection Directive 95/46/EC.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, executed in Strasbourg on 28 January 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans border data flows, executed in Strasbourg on 8 November 2001 have also been ratified by Ukrainian Parliament on 6 July 2010 ("**Convention on Automatic Processing of Personal Data**") and thus are fully effective in Ukraine.

General data protection issues are also regulated by the Constitution of Ukraine dated 28 June 1996, the Civil Code of Ukraine dated 16 January 2003 No 435 IV, the Law of Ukraine "On Information" dated 2 October 1992 No 2657 XII, Law of Ukraine "On Protection of Information in the Information and Telecommunication Systems" dated 5 July 1994 No. 80/94 VR and some other legislative acts.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DEFINITION OF PERSONAL DATA

Data Protection Law defines "personal data" as data or an aggregation of data on an individual who is identified or can be precisely identified.

DEFINITION OF SENSITIVE PERSONAL DATA

There is no definition of "sensitive personal data" as such envisaged by Ukrainian legislation.

At the same time, there is general prohibition to process personal data with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offences or conviction to criminal punishment as well as data relating to health or sex life of an individual.

Processing of the listed data is allowed if an unambiguous consent has been given by the personal data subject or based on exemptions envisaged by Data Protection Law (e.g. the processing is performed for the reasons of protection of vital interest of individuals, healthcare purposes, in course of criminal proceedings, anti-terrorism purposes, etc.).

NATIONAL DATA PROTECTION AUTHORITY

The State Service of Ukraine on Personal Data Protection ("**SSUPDP**").

REGISTRATION

The database containing personal data should be registered with the SSUPDP and the relevant record should be included into the State Register of Personal Data Databases.

Personal data owners which maintain their databases to secure and effect labour relations, as well as maintain personal data databases of the members of non-government, religious organizations, professional associations and political parties are released from mandatory registration of such personal data databases.

According to Data Protection Law as well as The Regulation on State Register of Databases Containing Personal Data approved by the Cabinet of Ministers of Ukraine the above registration shall be performed by the owner of personal data by means of submitting respective application to SSUPDP. The form of the application, as well as the order for filing the application has been approved by Ministry of Justice of Ukraine.

The Data Protection Law envisages that applications for the registration of a personal data database shall contain, inter alia, information as regards the owner of personal data; the name and place of location of database; the purpose of personal data processing; information on composition of personal data, information on third parties to whom the personal data are transferred, information on cross-border transfers of personal data, information on processors of database; confirmation as regards maintaining the security of personal data in the database.

SSUPDP takes a decision on registration of personal data database within 30 working days from the day of submission of application.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Personal data owners shall notify SSUPDP on any changes in information submitted thereto during registration of database within 10 business days following the day when the relevant changes occurred.

DATA PROTECTION OFFICERS

Legal entities shall establish a special department or appoint a responsible person (data protection officer) to organise the work related to protection of personal data during the processing thereof.

COLLECTION AND PROCESSING

The Data Protection Law provides for a requirement of obtaining the consent of personal data subjects on processing of their personal data. The consent of personal data subjects is determined by the Data Protection Law as their expression of will to allow the personal data processing in the form that enables a conclusion on granting such a consent. In some instances provided by Data Protection Law (e.g. legislative permission for processing of personal data, conclusion and execution of a transaction in favour of the personal data subject, protection of interests of the subject or owner of personal data) personal data of individuals may be processed without consent.

Pursuant to the Data Protection Law, as a general rule personal data subjects shall be informed, at the moment of collection of their personal data, of; the owner of their personal data; composition and content of their personal data being collected; their rights; purpose of their personal data collection; and the persons to whom their personal data will be transferred. However, in cases when the personal data of individuals have been collected based on the following grounds the personal data subjects shall be informed of the above within 10 working days from the moment of their personal data's collection:

- legislative permission of the owner of personal data on processing of personal data exclusively for the purposes of fulfilling its authorities;
- conclusion and execution of a transaction, in which the subject of personal data is a party or which has been concluded in favour of the subject of personal data or for taking actions, which preceded conclusion of a transaction at the request of the subject of personal data;
- protection of vital interests of the subject of personal data; or
- need to protect legitimate interests of the owner of personal data, third parties, except where a subject of personal data demands to stop processing of his/her personal data and the need in protection of personal data prevail over such interest.

In addition, the Data Protection Law provides the subject of personal data with the following rights:

- to be aware of the location of the database containing his/her personal data, the purpose and the title of the database, the address of the owner or user of the personal data or to obtain the mentioned information;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- to obtain information as regards the conditions of providing access to personal data, in particular, information on third parties, to which his/her personal data is transferred;
- to access his/her personal data;
- to obtain a reply within 30 calendar days from the date of receipt of his/her request, informing the individual whether his/her personal data is contained in the relevant database;
- to provide a reasonable request to change or destroy his/her personal data by any owner and processor of the personal data if the data is processed illegally or is inaccurate;
- to protect his/her personal data from unauthorised processing and accidental loss, elimination or damage with respect to intended encapsulation, not providing or the untimely providing of personal data, and also to protection from providing invalid or discrediting information regarding the individual;
- to appeal violations in the course of personal data processing to the SSUPDP or to the court;
- to introduce limitations as regards right on its personal data processing while giving the consent;
- to revoke its consent on personal data processing;
- to be aware of the mechanism of automatic processing of personal data;
- to be protected from the automated decision that has a legal effect; and
- to use the means of legal protection in the case of violation of rights to personal data.

The owner of the personal data can entrust processing of personal data to the processor of personal data under the written agreement between them. In this case the processor of personal data may process the personal data only for the purposes and in the volume provided by such agreement. The transfer of personal data to the processor of personal data can be allowed only by respective consent of personal data subject.

TRANSFER

In accordance with Data Protection Law the personal data may be transferred to foreign counterparties only on condition of ensuring appropriate level of protection of personal data by the respective state of transferee. Pursuant to the Data Protection Law, such states include member-states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine.

Personal data may be transferred abroad based on one of the following grounds:

- unambiguous consent of personal data subject;
- cross-border transfer is needed to enter into or perform a contract between the personal data owner and third party in favour of personal data subject;
- necessity to protect vital interests of the personal data subject's;

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

- necessity to protect public interest, establishing, fulfilling and enforcing of legal requirement; or
- appropriate guarantees of the personal data owner as regards non-interference in personal and family life of personal data subject.

SECURITY

The subjects of personal data relations are obliged to take appropriate technical and organisational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorised access. In this regard, any owner of personal data shall determine a special department or a responsible person to organise the work related to protection of personal data during the processing thereof.

Additionally, the Model Order of Personal Data Processing approved by the Ministry of Justice of Ukraine envisages general provisions as regards the processing of personal data in automated systems (the procedure of access by the personnel of personal data owners to the personal data within, automated system the necessity to protect the automated system with antivirus software and technical facilities preventing the leak of personal data) as well as processing of personal data in the form of card-files (the necessity to protect the card-files from unauthorised access, the procedure of formation of separate files containing personal data depending on the purpose of personal data processing).

The Data Protection Law also establishes that specific individuals – private entrepreneurs, doctors with an appropriate license, advocates and notaries – are obliged to personally ensure the protection of personal data owned by them.

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the appropriate state authority.

ENFORCEMENT

According to Data Protection Law SSUPDP is the state authority responsible for controlling the compliance with personal data protection legislation. Failure to comply with provisions of Data Protection Law can lead to responsibility prescribed by law.

Violation of personal data protection legislation may result to civil, criminal and administrative liability.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

If the violation has led to material or moral damages, the violator can be obliged by the court to reimburse them.

Code of Ukraine on Administrative Offenses envisages liability for the following actions:

- failure to notify or delay in providing notification of the subject of personal data on the owner of his/her personal data, composition and content of his/her personal data being collected, his/her rights, purpose of his/her personal data collection and the persons to whom their personal data will be transferred may lead to fine of up to EUR 638;
- failure to notify or delay in providing notification of the SSUPDP on personal data protection about change of information submitted for the state registration of personal data database may lead to the fine for up to EUR 638;
- deviation from the state registration of personal data database may lead to the fine for up to EUR 1594;
- non-observance of established procedure for protection of personal data in personal data database which led to unauthorised access to personal data may lead to the fine for up to EUR 1594;
- non-fulfilment of legal requirements of the officials of SSUPDP as regards elimination of violations in the sphere of personal data protection may lead to the fine for up to EUR 319.

The criminal liability, prescribed by the Criminal Code of Ukraine envisages fines for up to EUR 1625 or correctional works for a term of up to two years, or up to six months arrest, or up to three years of limitation of freedom for the illegal collection, storing, use, elimination, spreading of confidential information about individual or illegal change of such information.

ELECTRONIC MARKETING

Ukrainian legislation does not specifically regulate the area of electronic marketing. However, in case, when electronic marketing involves processing of individuals personal data, it should take place in compliance with requirements of Ukrainian data protection legislation.

Considering requirements of the Data Protection Law outlined above, in order for the use of individuals personal data for electronic marketing purposes, it is required to obtain appropriate consent of individual which would reflect processing of his/her personal data for such purposes.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There is no specific legislation regulating the sphere of online privacy in Ukraine. However, the Data Protection Law applies to the extent online activities involving processing of personal data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

62. UNITED STATES

CONTRIBUTION DETAILS

Jim Halpert
Partner and Head of US Information Law Team
T +1 202 799 4441
jim.halpert@dlapiper.com

Kate Lucente
Associate
T +1 813 222 5927
kate.lucente@dlapiper.com

Jennifer Kashatus
Of Counsel
T +1 202 799 4448
Jennifer.kashatus@dlapiper.com

LAW

The United States has about 20 sector specific or medium specific national privacy or data security laws, and hundreds of such laws among its 50 states. (California alone has more than 25 state privacy and data security laws). These laws address particular problems or industries. They are too diverse to summarize fully in this volume

In addition, the large range of companies regulated by the Federal Trade Commission ("**FTC**") are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement minimal data security measures or fail to live up to promises in privacy policies.

DEFINITION OF PERSONAL DATA

Varies widely by regulation.

DEFINITION OF SENSITIVE PERSONAL DATA

Varies widely by regulation.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

NATIONAL DATA PROTECTION AUTHORITY

No official national authority. However, the FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (e.g. for telemarketing, spamming, and children's privacy). The FTC uses its general authority to prevent unfair and deceptive trade practices to bring enforcement actions against inadequate data security measures, and inadequately disclosed information collection, use and disclosure practices. State Attorneys General typically have similar authority and bring some enforcement actions.

In addition, a wide range of sector regulators, particularly those in the health care and financial services sectors, have authority to issue and enforce privacy regulations.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

With the exception of entities regulated by HIPAA, there is no requirement to appoint a data protection officer, although appointment of a chief privacy officer and an IT security officer is a best practice among larger organisations.

COLLECTION AND PROCESSING

US privacy laws and self-regulatory principles vary widely, but generally require pre-collection notice and an opt out for use and disclosure of regulated personal information.

Opt in rules apply in special cases involving information that is considered sensitive under US law, such as for health information, use of credit reports, personal information collected online from children under 13 (see below for the scope of this requirement), video viewing choices, and telecommunication usage information. The FTC interprets as a "deceptive trade practice" failing to obtain opt in consent if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was collected.

States impose a wide range of specific requirements, particularly in the employee privacy area.

The US regulates marketing communications extensively, including telemarketing, fax marketing and email marketing (which is discussed below).

TRANSFER

No geographic transfer restrictions apply in the US, except with regard to accountants transferring tax preparation materials. The Commerce Clause likely bars US states from imposing data transfer restrictions and there are no other such restrictions in US national laws.

By contrast, some European data protection authorities take the position that personal data transferred to the United States under the US EU Safe Harbor principles may not be transferred outside the US without another valid legal basis.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

SECURITY

Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (e.g. health or financial information, telecommunications usage information, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for data elements that trigger security breach notice requirements. For example, Massachusetts has enacted regulations, which apply to any company that collects or maintains sensitive personal information on Massachusetts resident. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program; the regulations also set forth the minimum components of such program. HIPAA regulated entities have much more extensive data security requirements, and some states impose further security requirements (e.g. for payment card data, for social security numbers, or to employ secure data destruction methods). HIPAA security regulations apply to so-called "covered entities" such as doctors, hospitals, insurers, pharmacies and other health-care providers, as well as their "business associates" which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity.

BREACH NOTIFICATION

Security breach notification requirements are a US invention. 46 US states and most US territories require notifying state residents of a security breach involving residents' name plus a sensitive data element – typically, social security number, other government ID number, or credit card or account number in combination with any security code or password that would permit access to a financial account. Notice of larger breaches is typically required to be provided to credit bureaus, and in minority of states, to State Attorneys Generals, and in rare cases to other state officials. National laws require notification in the case of breaches of health care information, breaches of information from financial institutions, and breaches of government agency information.

ENFORCEMENT

Violations are generally enforced by the FTC, State Attorneys General, or the regulator for the industry sector in question. Civil penalties are generally significant. In addition, some privacy laws (for example, credit reporting privacy laws, electronic communications privacy laws, video privacy laws, call recording laws, cable communications privacy laws) are enforced through class action lawsuits for significant statutory damages and attorney's fees, and defendants can be sued for actual damages for negligence in mishandling personal information such as payment card data.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

E-mail: The CAN-SPAM Act is a federal law that applies labelling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender's contact information, and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. Not only the FTC and State Attorneys General, but also ISPs and corporate email systems can sue violators. Furthermore, knowingly falsifying the origin or routing of a commercial email message is a federal crime.

Text Messages: Federal and state regulations apply to the sending of marketing text messages to individuals. Generally, express, opt-in consent is necessary to send marketing text messages and applicable regulations also specify the form of consent.

Telemarketing: In general, federal law applies to most telemarketing calls and programs, and a state's telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing. For example, national ("federal") and state rules address calling time restrictions, honouring do-not-call registries and opt-out requests, mandatory disclosures to be made during the call, requirements for completing a sale, executing a contract or collecting payment during the call, restrictions on the use of auto-dialers and pre-recorded messages, and record keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls.

Callers generally must scrub their calling lists against both a national and multiple state do-not-call registries, as it is prohibited to place a telemarketing call to a number listed in a do-not call registry unless a specific exemption applies. The national do-not-call rules (and several state rules), for example, exempt calls to existing business customers who have purchased a product or service in the last 18 months from the company on whose behalf the call is placed, as long as the customer has not specifically opted out of receiving telemarketing calls from the company. The use of auto-dialers to send pre-recorded messages generally requires affirmative opt-in consent of the recipient.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

Fax Marketing: Federal law and regulations generally prohibit the sending of unsolicited advertising by fax without prior, express consent. Violations of the law are subject to civil actions and have been the subject of numerous class action lawsuits. The law exempts faxes to recipients that have an established business relationship with the company on whose behalf the fax is sent, as long as the recipient hasn't opted out of receiving fax advertisements and has provided their fax number "voluntarily," a concept which the law specifically defines. The law also requires that each fax advertisement contain specific information, including (i) a "clear and conspicuous" opt out method on the first page of the fax; (ii) a statement that the recipient may make a request to the sender not to send any future faxes and that failure to comply with the request within 30 days is unlawful; and (iii) a telephone number, fax number, and cost-free mechanism to opt-out of faxes, which permit consumers to make opt-out requests 24 hours a day, seven days a week.

ELECTRONIC PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

Cookies: There is no specific federal or state law that regulates the use of cookies, web beacons, Flash LSOs and other similar tracking mechanisms. However, undisclosed online tracking of customer activities poses class action risk. The use of cookies and similar tracking mechanisms should be carefully and fully disclosed in a website privacy policy. Furthermore, it is a best practice for websites that allow behavioural advertising on their websites to participate in the Digital Advertising Alliance code of conduct, which includes displaying an icon from which users can opt-out of being tracked for behavioural advertising purposes.

Location Data: Privacy requirements of location-based apps and services is in flux and is a subject of extensive interest and debate. Federal Communications Commission regulations govern the collection and disclosure of location information by telecommunications carriers, including wireless carriers. Further, any location service that targets children under the age of 13 or has actual knowledge that it is collecting location information from children under age 13 must comply with the requirements of the Children's Online Privacy Protection Act (COPPA) Rules – including obtaining prior verifiable parental consent in most circumstances. Both the Federal Trade Commission and California Attorney General's Office have issued best practices recommendations for mobile apps and mobile app platforms, and the California Attorney General has entered into an agreement with major app platforms in which they promise to prompt mobile apps to post privacy policies. Furthermore, a Department of Commerce-led multi-stakeholder negotiation to develop a code of conduct for mobile app privacy is well underway.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

63. URUGUAY

CONTRIBUTION DETAILS

Estudio Bergstein
www.bergsteinlaw.com

Jonás Bergstein
Partner
jbergstein@bergsteinlaw.com

Gabriel Egjenberg
Senior Associate
T +598 2 901 2448
gejenberg@bergsteinlaw.com

LAW

Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 2009) (the "**Act**").

DEFINITION OF PERSONAL DATA

Any kind of information related to a person or legal entity identified or identifiable.

DEFINITION OF SENSITIVE PERSONAL DATA

Any kind of personal data evidencing: racial or ethnic origin, political preferences, religious or moral beliefs, trade union membership and any kind of information concerning health or sexual life.

NATIONAL DATA PROTECTION AUTHORITY

("**URCDP**", Unidad Reguladora de Control y Actos Personales ("**Data Protection Authority**").

REGISTRATION

Every database must be registered with the Data Protection Authority in Uruguay if the information contained in the database is gathered or obtained through means, mechanisms or sources located in Uruguay.

The database must be registered by filing mandatory forms which must be signed by a representative of the company which owns the data base.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

DATA PROTECTION OFFICERS

No requirement to appoint a data protection officer.

COLLECTION AND PROCESSING

In order to collect the information which is contained in the database, the data processor should obtain prior documented consent from the individual or entity whose information is being processed. Documented consent is not required in the following cases:

- personal data obtained from public sources;
- personal data obtained by public bodies to comply with legal obligations;
- personal data limited to domicile, telephone number, ID number, nationality, tax number, corporation name;
- personal data obtained based on a contractual or professional relationship, which is necessary to perform the contract or the development of the professional services to be rendered; and
- personal data obtained by individuals or corporations for their personal and exclusive use.

The personal data processed cannot be used for secondary purposes different from those that have justified the acquisition of the information. It is understood that legitimate reasons (i.e. reasons which are not against the law) must pre-exist and underlay the processing of the personal information. The Act further establishes that once the reasons to process the personal information are no longer present, the personal information must be deleted.

TRANSFER

Personal data can only be transferred to a third party:

- for purposes directly related to the legitimate interests of the transferring party and the transferee; and
- with the prior consent of the data subject. However, such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer, as well as of the identity of the recipient.

However, the prior consent of the data subject is not necessarily required when the personal data to be transferred is limited to: name, surname, identity card number, nationality, address, and date of birth.

The purpose and proper identification of the transferee must be included in the request for consent addressed to the data subject. Evidence of the data subject's consent must be kept in the files of the data processor.

If the data subject's consent is not obtained within ten business days (counted from the receipt of the communication from the data processor asking for the consent), it will be construed that the data subject did not consent to the transfer of the data.

Upon the transfer, the data processor will remain jointly and severable liable for the compliance of the recipient's obligations under the Act.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

The Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of protection (according to European standards). However, the Act allows international transfer to unsafe countries or entities, when the data subject consents to the transfer (such consent must be given in writing), or when the guarantees of adequate protection levels arise from "contractual clauses", and "self-regulation systems". The international data transfer agreement must provide for the same levels of protection which are effective under the laws of Uruguay.

In the case of a cross border transfer within a group of companies, Uruguayan laws establish that the international transfer will be lawful without any authorisation whenever the recipient branch has adopted a conduct of code duly registered with the local URCDP.

The international transfer of personal data between headquarters and their respective branches or subsidiaries is authorised when the headquarters and their branches have a code of conduct (such as an inter-company agreement) duly filed with URCDP.

SECURITY

Data processors must implement appropriate technical and organisational measures to guarantee the security and confidentiality of the personal data. These measures should be aimed at preventing the loss, falsification, and unauthorised treatment or access, as well as at detecting information that may have been lost, leaked, or accessed without authorization.

It is prohibited to register personal data in databases which do not meet technical safety conditions.

BREACH NOTIFICATION

In case the data processor detects a breach of security measures, and if the consequences of the breach could substantially affect the rights of the data subject, and/or the rights of any other agent or person involved, the data processor should report the facts to the persons involved.

ENFORCEMENT

The URCDP is responsible for enforcement of the Act. In the context of its powers, the URCDP has broad investigatory powers, including audit and inspection rights, and subpoena, search and seizure authority.

The URCDP has the authority to impose penalties against the data processor in the following order: warning, admonition, fines up to USD 60,000, suspension of the database for five days, closure of the database.

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Costa Rica
Cyprus
Czech Republic
Denmark
DIFC
Egypt
Finland
France
Germany
Gibraltar
Greece
Honduras
Hong Kong
Hungary
India
Indonesia
Ireland
Italy
Japan
Lithuania
Luxembourg
Malaysia
Malta
Mauritius
Mexico
Monaco
Morocco
Netherlands
New Zealand
Norway
Pakistan
Panama
Philippines
Poland
Portugal
Romania
Russia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Trinidad and Tobago
Turkey
UAE
UK
Ukraine
United States
Uruguay

ELECTRONIC MARKETING

The Act will apply to most electronic marketing activities, as these activities typically involve the processing and use of personal data (e.g. an email address is likely to be "personal data" for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing, but grants personal data owners (individuals or companies) with the right to demand the deletion or suppression of their data from the marketing database.

Personal data may be used and processed for marketing purposes when the personal data was either obtained from public documents, provided by the data subject or when prior consent has been gathered.

ONLINE PRIVACY (INCLUDING COOKIES AND LOCATION DATA)

There are no provisions that specifically address online tracking or geolocation data. However, the general principles of the Act apply: the personal data processed cannot be used for purposes other than those that justified the acquisition of the data; and when the reasons to process the personal information have expired, the personal information must be deleted.

If you have finished with this document, please pass it on to other interested parties or recycle it, thank you.

www.dlapiper.com

This handbook is provided to you as a courtesy, and it does not establish a client relationship between **DLA Piper** and you, or any other person or entity that receives it. It provides a general overview of the data protection regime currently in force in 63 jurisdictions. It is a general reference document and should not be relied upon as legal advice. The application and effect of any law or regulation upon a particular situation can vary depending upon the specific facts and circumstances, and so you should consult with a lawyer regarding the impact of any of these regimes in any particular instance.

DLA Piper and the other contributing law firms accept no liability for errors or omissions appearing in the handbook and, in addition, **DLA Piper** accepts no liability at all for the content provided by the other contributing law firms. Please note that privacy and information law is dynamic, and the legal regime in the countries surveyed could change.

No part of this publication may be reproduced or transmitted in any form without the prior consent of the **DLA Piper**.

Copyright © 2013 DLA Piper. All rights reserved. | MAR13 | 2514176