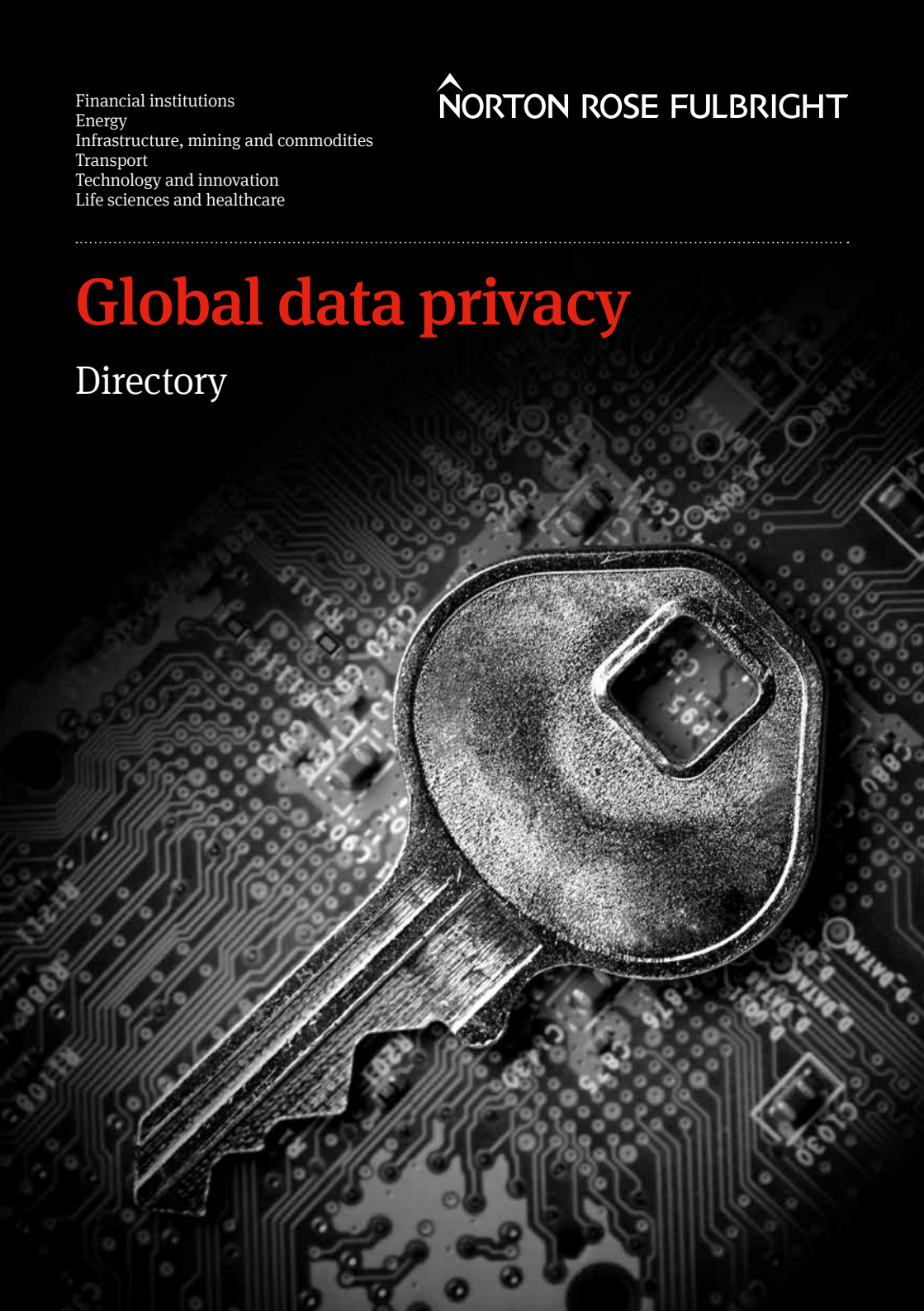
Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Global data privacy

Directory



Attorney advertising

Global data privacy

Directory

A Norton Rose Fulbright directory
July 2014

Norton Rose Fulbright is a global legal practice. We provide the world's pre-eminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers based in over 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Contents

Introduction	**07**
Our thanks to	**08**
Europe and Russia	**11**
Andorra	14
Austria	16
Belarus	18
Belgium	20
Bulgaria	21
Croatia	23
The Republic of Cyprus	25
Czech Republic	27
Denmark	29
Estonia	31
Finland	33
France	35
Germany	37
Gibraltar	39
Greece	42
Hungary	44
Iceland	46
Ireland	48
Italy	50
Kazakhstan	52
Latvia	55
Lithuania	57
Luxembourg	59
Malta	60
The Netherlands	62
Norway	63
Poland	64
Portugal	66
Romania	67
Russia	69
Serbia	71
Slovak Republic	73
Slovenia	76
Spain	78
Sweden	80
Switzerland	82
Turkey	85
United Kingdom	87
Ukraine	88
The Americas	**91**
Argentina	92
Brazil	94
Canada	96
Chile	99
Colombia	102

Mexico 104
Uruguay 107
United States 109
Venezuela 115
Africa 117
Angola 118
Ghana 120
Kenya 121
Malawi 123
Mozambique 124
Nigeria 125
South Africa 126
Tanzania 127
Uganda 129
Zambia 131
Zimbabwe 133
Middle East 135
Afghanistan 136
Bahrain 137
Egypt 140
Iran 143
Iraq 145
Israel 147
Jordan 150
Kuwait 152
Lebanon 154
Oman 156
Pakistan 158
Palestine 163
Qatar 165
Saudi Arabia 167
Syria 169
United Arab Emirates 171
Asia Pacific 175
Australia 176
China 177
Hong Kong 179
India 180
Indonesia 181
Japan 183
Malaysia 184
New Zealand 186
Philippines 188
Singapore 189
South Korea 191
Taiwan 192
Thailand 193
Vietnam 194
Contacts 197

Introduction

International data privacy legislation and increasing consumer demand for protection of personal information mean that personal information must be now gathered, processed and stored in accordance with applicable data privacy laws.

This directory is designed to give businesses a brief overview of the data privacy legislation applicable in key jurisdictions around the world, and any restrictions imposed on the transfer of personal data. This will be of interest to those multinationals which process data overseas or which are considering exporting data overseas.

The Norton Rose Fulbright data privacy team comprises lawyers focused on data protection and privacy. In countries where we do not have offices, we work with a network of specialist data protection and privacy lawyers in correspondent firms. This gives our clients access to information globally through Norton Rose Fulbright. We advise on compliance, data relocation, data breaches and data products, and marketing.

The information contained in this directory is accurate and up-to-date as at July 2014. It is not a substitute for legal advice. If you would like to discuss any of the issues covered, please get in touch with us.

Our thanks to

the law firms listed below for their help in preparing this directory.

Europe

Arqués Ribert Junyer Advocats	Andorran law
Herbst Vavrovsky Kinsky Rechtsanwälte GmbH	Austrian law
Sorainen	Belarusian law
Boyanov & Co.	Bulgarian law
Divjak, Topić & Bahtijarević	Croatian law
Aristodemou Loizides Yiolitis LLC (Harneys)	law of the Republic of Cyprus
Bech-Bruun	Danish law
Sorainen	Estonian law
Waselius & Wist	Finnish law
Hassans	Gibraltar law
Burai-Kovács & Partners	Hungarian law
LOGOS	Icelandic law
Matheson	Irish law
Sorainen	Latvian law
Sorainen	Lithuanian law
Wildgen Partners in Law	Luxembourgian law
Fenech and Fenech Advocate	Maltese law
Wiersholm	Norwegian law
Garrigues	Portuguese law
Vilau & Mitel	Romanian law
BDK Advokati Attorneys at Law	Serbian law
Beatow Partners	law of the Slovak Republic
Jadek & Pensa	Slovenian law
Garrigues	Spanish law
Mannheimer Swartling	Swedish law
Niederer Kraft & Frey	Swiss law
Hergüner, Bilgen, Özeke	Turkish law
Egorov Puginsky Afanasiev & Partners	Ukrainian law

The Americas

Beretta Godoy	Argentinian law
Veirano Advogados	Brazilian law
Guerrero, Olivos, Novoa y Errázuriz	Chilean law
Barrers, Siqueiros y Torres Landa, S.C.	Mexican law
Estudio Ferrere	Uruguayan law

Africa

Miranda Correia Amendoeira & Associados	Angolan law
Fugar & Co	Ghanaian law
Kaplan & Stratton	Kenyan law
Savjani & Co	Malawian law
Mozambique Legal Circle	Mozambican law
Udo Udoma & Belo-Osagie	Nigerian law
Shonubi Musoke & Co	Ugandan law
Corpus Legal Practitioners	Zambian law
Gill Godlonton & Gerrans	Zimbabwean law

The Middle East

Law Offices of A. Rahman Rahimghiyasa	Afghan law
ASAR – Al Ruwayeh & Partners	Bahraini law
Sharkawy & Sarhan Law Firm	Egyptian law
Atieh Associates	Iranian law
Serge Airut	Iraqi law
Herzog Fox & Neeman	Israeli law
Ali Sharif Zu'bi Advocates & Legal Consultants	Jordanian law
ASAR Legal	Kuwaiti law
Moghaizel Law Office	Lebanese law
Said Al Shahry Law Office	Omani law
Vellani & Vellani	Pakistani law
Al-Zubi Law Office	Palestinian law
Arab Law Bureau	Qatari law
Sarkis Attorneys at Law	Syrian law

Asia Pacific

Fortitude Law Associates	**I**ndian law
Atsumi & Sakai	Japanese law
Zaid Ibrahim & Co	Malaysian law
Tompkins Wake Lawyers	New Zealand law
S**iguion Reyna Montecillo & Ongsiako**	Philippine law
Barun Law South	Korean law
Russin & Vecchi	Taiwan law
Vision & Associates Legal	Vietnam law

Europe and Russia

Definitions

The definitions below are applicable to the following Europe and Russia section of the 2014 directory:

Binding Corporate Rules or **BCRs** means a global set of legally enforceable intra-group rules that achieve legal and practical compliance with the requirements of the EU Data Protection Directive 95/46 EC as defined in the EU Article 29 Working Party Working Document WP74 (please see this link for further information: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf)

Convention 108 means the Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981 European Treaty Series, No. 108.

EU Data Protection Directive 95/46 EC means the European Union directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EU Directive on Privacy and Electronic Communications 02/58 EC means the European Union directive on the processing of personal data and the protection of privacy in the electronic communications sector (as amended by Directive 2009/136).

European Economic Area or **EEA** consists of Iceland, Liechtenstein, Norway and the European Union member states.

EU Model Clauses means the following model contractual clauses adopted by the European Commission, transfers under which are deemed to have an adequate level of data protection:

(a) Decision 2001/497/EC on standard contractual clauses for the transfer of personal data from controllers to controllers established in third countries;

(b) Decision 2004/915/EC on the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries; and

(c) Decision 2010/87/EU on updating the standard contractual clauses for the transfer of personal data from controllers to processors established in non-EU countries.

EU/US Safe Harbour means the data protection compliance self-certification system open to certain US companies, transfer under which the EU Commission has deemed to provide an adequate level of data protection.

White Listed countries means the list of countries approved by the EU Commission as having an adequate level of data protection. As of July 31, 2014 the White List includes: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay.

Andorra

Although Andorra is not a member of the EU and so has not implemented the EU directives, Andorra has comprehensive data privacy legislation that bears similarities to the EU regime. The Andorran data protection regime applies to both private and public entities, and regulates how a data controller collects, processes and uses a data subject's personal data.

Applicable legislation:

A number of pieces of legislation and regulation form the Andorran data protection system.

These include:

- The Qualified Law of Personal Data Protection 15/2003, of 18th December; and
- A Decree of 9th June 2010, which approved Regulations of the Andorran Personal Data Protection Agency and fleshed out in greater detail the requirements of the Qualified Law of Personal Data Protection 15/2003, of 18th December.

The Andorran Personal Data Protection Agency supervises compliance with data protection standards and manages a register of data controllers. The Personal Data Protection Agency is also empowered to impose fines and penalties.

Protected data:

Andorran data protection law protects personal data. This is defined as all information relating to individuals (not legal entities) who are or can be identified from the information and who are susceptible to adverse consequences from its use.

Personal data may, however, be subject to less stringent controls than normal in fields such as: state security, defence and the investigation and prevention of criminal activities. Personal data included in a private individual's files for purposes such as use in a diary or schedule, may also be exempt.

A higher level of protection is accorded to sensitive information. This includes personal data revealing political or trade union membership, religious beliefs and information concerning a person's health, sex life or ethnic origin.

Restrictions on transfer of data offshore:

Principle
Personal data can only be transferred to third countries which guarantee a level of data protection which is at least as protective as the Andorran data protection regime.

EU/EEA and White List
Under the Andorran Qualified Law of Personal Data Protection 15/2003, of 18th December, there is a presumption that EU member states, members of the EEA, White Listed countries and other countries listed by the Andorran Data Protection Agency offer an equivalent level of protection. The transfer of personal data to these countries does not require any authorisation from the Andorran Data Protection Agency.

Other countries
Data can be exported to a third country outside the EU, the EEA, the White Listed countries and the Andorran Personal Data Protection Agency listed countries, if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest. Where a condition is met, the Andorran Data Protection Agency's authorisation is not required.

EU Model Clauses can also be used to achieve a compliant export to third countries, but those clauses must be compulsory and approved by the Andorran Data Protection Agency prior to export. The transfer of personal data between Andorran and third country enterprises is permitted only where the Andorran Data Protection Agency authorises the transfer and is satisfied with the EU Model Clauses or BCRs clauses included in the transfer agreement.

Austria

Austria has comprehensive legal rules regarding data protection consistent with the applicable EU Data Protection Directive 95/46 EC.

Applicable legislation:

Austria has implemented the EU Data Protection Directive 95/46 EC through the Data Protection Act 2000, as amended. It applies both to the private and public sector. Austria has also implemented the EU Directive on Privacy and Electronic Communications 02/58 EC through the Telecommunications Act 2003.

Austrian data protection law applies to the use of personal data in Austria, irrespective of the place of residence or corporate seat of the respective data controller, if personal data is processed in the context of an establishment in Austria (except for transient purposes). In addition, Austrian data protection law applies to the use of data outside of Austria (but within the EEA) if processing is made for the purpose of an Austrian head or branch office of the data controller. Protection is granted for both natural and legal persons.

The Austrian Data Protection Authority (DPA) is responsible for keeping the Data Processing Register of data controllers and their processing activities (data applications), which is publicly accessible. The DPA has the power to: investigate suspected violations of data protection law; expressly prohibit a data processing activity; issue recommendations to the data controller to re-establish compliance with data protection law; and, take steps to induce a criminal court or administrative authority to initiate proceedings.

Protected data:

The Data Protection Act 2000 grants everybody a constitutional right to the secrecy of his personal data to the extent that the relevant person has an interest that deserves this protection.

Personal Data is defined as any information relating to an identified or identifiable data subject. It includes facts that can be associated with a person, such as a person's name, date of birth, address, salary size, as well as value judgements. Anonymous data is not protected.

'Everybody' means data subjects whose data is processed or transferred. The concept of a 'data subject' is wide in Austria, comprising not only natural persons but also legal persons and groups of natural persons, such as partnerships.

In accordance with the EU Data Protection Directive 95/46 EC, a higher degree of protection applies to sensitive data. Sensitive data is any information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs as well as health or sex life. Sensitive data may only be used on the basis of specific reasons laid down in the Data Protection Act 2000. Furthermore, any data processing activity involving sensitive data, data on creditworthiness and data relating to criminal or administrative offences is subject, in principle, to prior approval by the DPA.

Restrictions on transfer of data offshore:

Transfer of data to a recipient outside Austria may require the prior approval of the DPA.

EEA, White List and Safe Harbour

Approval is not required to transfer data within the EEA or to White Listed countries. Transfers to EU/US Safe Harbour certified recipients in the USA do not require the prior approval of the DPA.

Other countries

In all other cases, the data controller needs to seek the prior approval of the DPA for the intended transfer.

Where the transfer is between a group of companies under BCRs or where standard EU Model Clauses are used, the data controller will still need to apply for approval. However, approval is generally granted in these situations and often more quickly.

Belarus

The Belarusian regulatory framework for data protection is the Information Protection Law.

Applicable legislation:

Two key pieces of legislation set out the data protection rules applicable in Belarus. These are:

(1) The Law of the Republic of Belarus No. 455-Z of 10 November 2008 "On Information, Informatisation and Information Protection" (the Information Protection Law). A revised version of the Information Protection Law entered into force on 11 April 2014.

(2) The Law of the Republic of Belarus No. 418-Z of 21 July 2008 "On the Population Register" (the Population Register Law), as amended, which regulates the inclusion and sharing of personal data extracted from the Belarusian Population Register (the Register).

There are two authorities primarily occupied with overseeing compliance with the Information Protection Law. They are: i) the Operational-Analytical Center under the President of the Republic of Belarus; and ii) the Ministry of Communications and Informatisation. Non-compliance with the norms of the Information Protection Law is subject to administrative and criminal charges (generally fines), which are imposed by the competent courts.

Protected data:

General principle

The Information Protection Law contains a general requirement that personal data is only collected, processed, stored and used with the consent of the individual it concerns. Since April 2014, an individual's consent must be in writing.

Personal data

In Belarus, personal data is classified as one of three types: "basic", "additional" and "other identifying information".

Basic data is defined in a closed list of information, which includes, inter alia, a person's name, date of birth and nationality. Additional data is also defined by a closed list, which includes information concerning person's education, tax obligations/status and military record.

"Basic" and "additional" personal data can be entered into the Register, which is a state

centralised automatic information system containing the personal data of citizens and permanent residents of the Republic of Belarus. The Register is maintained by state entities and serves as an up-to-date record of individuals in Belarus available to state bodies, entities and individuals. A data subject's consent is not required to add information to the Register or for the Ministry of Internal Affairs (administrator of the Register) to disclose information to recipients authorised by the legislation, such as notaries in specific cases.

There is no specific concept of sensitive personal data in the Republic of Belarus with stricter processing conditions. Additional data is not subject to stricter processing conditions and is not treated in a specific way. Nevertheless, basic data and additional data as well as any comments noted in the Register are confidential.

Restrictions on transfer of data offshore:

Belarusian legislation does not specifically regulate the export of personal data offshore but the general requirement of individual's consent would apply in this situation.

Belgium

Belgium has rules on data protection consistent with the principles contained in the EU Data Protection Directive 95/46 EC. Compliance with these rules is supervised by the Belgian Privacy Commission to which the processing of personal data must be notified.

Applicable legislation:

Data Protection Act

Belgian data protection legislation is based on the EU Data Protection Directive 95/46 EC which has been implemented in Belgium by the Act of 8 December 1992 on Privacy Protection in relation to the Processing of Personal Data, as amended by the Act of 11 December 1998 (the Data Protection Act). In addition, the Royal Decree of 13 February 2001 contains further implementing provisions. The Act of 26 February 2003 adapted the Privacy Commission's statute, composition and competences and established the Commission's Sector Committees.

Protected data:

The Data Protection Act protects "personal data" which includes 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 by one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Restrictions on transfer of data offshore:

The Data Protection Act only contains restrictions in relation to transfers outside the European Economic Area. Subject to certain exceptions, such transfers can only take place if the conditions as set out in the Data Protection Act are complied with and, in addition, the country in question guarantees an adequate level of protection.

Bulgaria

Bulgarian data protection rules are compliant with the principles laid down in the EU Data Protection Directive 95/46 EC.

Applicable legislation:

Bulgaria has implemented the EU Data Protection Directive 95/46 EC through the Personal Data Protection Act dated 4 January 2002, as amended (the PDPA).

Bulgaria has also implemented the EU Directive on Privacy and Electronic Communications 02/58 EC through the Electronic Communications Act 2007, as amended (the Electronic Communications Act).

The Commission for Personal Data Protection (the CPDP) supervises the application of data protection rules in Bulgaria. Matters of electronic communications are supervised by the Communications Regulation Commission.

The CPDP can sanction violations of the PDPA with various financial penalties ranging between BGN 500 (approx. € 250) and BGN 200,000 (approx. € 100,000), depending on the severity of the violation.

A provider of public electronic communications networks and/or services that fails to comply with personal data protection obligations in the field of electronic communications could be fined by the Communications Regulation Commission. Financial penalties range between BGN 1,000 – BGN 40,000 (approx. € 500 – € 20,000), depending on the severity of the violation

Protected data:

Personal data is any information relating to a natural person who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more specific factors.

A special degree of protection applies to “sensitive information” relating to a person’s race, ethnic origin, political, religious or philosophical views, political or union membership, sex preference, health or genetic information. Processing sensitive information is generally prohibited, subject to limited exceptions.

Restrictions on transfer of data offshore:

EEA and White List

The PDPA allows transfer within the EEA and to countries which have been White Listed without the need for approval.

Other countries

Data can be exported to a country outside the EEA and the White Listed countries, if EU Model Clauses are used in the transfer agreement with the data recipient to achieve an adequate level of data protection. This can also be carried out without the need for approval.

Otherwise, data can only be exported to third countries after the Bulgarian Commission for Personal Data Protection grants its explicit approval and if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest.

Croatia

Croatia has a comprehensive data protection legislative regime that complies with the EU data protection directives on data privacy. Personal data protection is also a constitutional right under the Croatian constitution.

Applicable legislation:

A number of pieces of legislation and regulation form the Croatian data protection system.

These are:

(1) The Act on Personal Data Protection (CAPDP), which implements the EU Data Protection Directive 95/46 EC and the EU Directive on Privacy and Electronic Communications 02/58 EC. The CAPDP regulates the personal data protection of natural persons and applies to both the public and private sector. It does not apply to personal data processing conducted by natural persons for personal or private purposes.

(2) Article 37 of the Constitution of the Republic of Croatia, which guarantees personal data protection.

Two regulations also regulate personal data processing in Croatia:

(i) the 'Regulation on the method of maintaining records on personal data filing system and the form of such records'; and

(ii) the 'Regulation on the manner of storing and providing technical protection for the special categories of personal data'.

The Croatian Personal Data Protection Agency (the Agency) acts as the supervisory authority for personal data protection. Where data protection law has been breached, the Agency may institute criminal or misdemeanour proceedings (these are proceedings for minor offences sanctioned by fines) before the competent courts.

Protected data:

Personal data means 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.

Higher restrictions apply to the processing of special categories of personal data pertaining to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health or sex life as well as personal data regarding criminal and misdemeanour proceedings in relation to the data subject. These special categories of data may be collected and processed only in exceptional cases prescribed by the CAPDP (for example, with the consent of the data subject and for the purpose of protecting the life or physical integrity of the data subject.)

Restrictions on transfer of data offshore:

EEA and White List

Transfer of personal data to countries within the EEA or to White Listed countries does not require authorisation.

Other countries

Data can be exported to a third country outside the EEA and the White Listed countries, if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest.

Data can also be exported to a third country if the data controller adequately ensures that the data subject's data, privacy and fundamental freedoms will be protected, by entering into a transfer agreement that the Agency has approved. EU Model Clauses can be used in this transfer agreement, if they specify the purpose of the data collection.

The prior approval of the Agency is not generally required to export to a third country. However, where the destination country is reasonably suspected to lack an adequate level of data protection, the data controller must obtain authorisation from the Agency.

The Republic of Cyprus

The Republic of Cyprus has implemented the EU Data Protection Directive 95/46 EC. The national data protection regime protects against the unauthorised and illegal use, recording or collection of personal information which relates to an individual.

Applicable legislation:

The Republic of Cyprus has implemented the EU Data Protection Directive 95/46 EC through the Processing of Personal Data (Protection of Individuals) Law of 2001, as amended. This key legislation is supported by the Data Processing (Permits and Fees) Regulations 2002 and the Regulation of Electronic Communications and Postal Services Law of 2004. The Constitution of the Republic of Cyprus also provides an individual with the right to respect for his private and family life and to the secrecy of his correspondence and other communication.

The local Data Protection Authority in Cyprus is the Commissioner for the Protection of Personal Data (the Commissioner), which supervises compliance with data protection standards and authorises processing activities. It can also impose administrative fines, issue warnings and report contraventions of the law.

Protected data:

Personal data is defined as any information from which a living natural person (the Data Subject) may be identified, directly or indirectly, and in particular by reference to a personal identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, political or social identity. Consolidated data of a statistical nature, from which the Data Subject cannot be identified is not deemed to be personal data.

Sensitive personal data includes data concerning racial or ethnic origin, political convictions, religious or philosophical beliefs, participation in an organisation or trade union, health, sex life, sex orientation and criminal prosecutions or convictions.

Restrictions on transfer of data offshore:

EEA and White List

Data may be transferred freely within the European Union, to states within the EEA, and to White Listed countries. No prior consent of the Commissioner is required.

Other countries

Personal data can usually only be exported to other third countries if a licence has been granted by the Commissioner.

The Commissioner issues licences only where he considers that the destination country ensures an adequate level of protection, in light of factors such as the nature of the data, the purpose and duration of the processing, the relevant general and special rules of law in the destination country, and the final destination of the data.

Data can be exported to a third country that does not adequately protect data on an exceptional basis, if the Commissioner consents and one or more of a number of specified conditions is met. These include that the Data Subject explicitly consents, the transfer is necessary for the performance of a contract for the Data Subject and/ or the transfer is necessary to serve an important public interest.

Furthermore, the Commissioner may also allow the transfer of data to a country which does not have a satisfactory level of protection, if the data controller puts in place sufficient safeguards to protect the Data Subject's privacy and fundamental rights. This can be achieved by using appropriate contractual clauses, such as EU Model Clauses, in the transfer agreement.

Czech Republic

The Czech Republic, as a member of the European Union, has implemented the system of data protection introduced by the EU Data Protection Directive 95/46 EC into national law. The Czech regulatory framework seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union.

Applicable legislation:

The Protection of Personal Data Act (no. 101/2000 Coll.) (the Act)

The Act regulates the rights and obligations that apply to the processing of personal data and specifies the conditions under which personal data may be transferred to other countries.

The Act applies to personal data that is processed by state authorities and other public authorities, as well as natural and legal persons. The Act applies to the processing of all personal data, whether by automatic or other means.

The Office for Personal Data Protection, which was established by the Act, exercises the competence of a supervisory authority for personal data protection.

In addition to the Act, there are other laws regulating various aspects of the system of personal data protection.

Protected data:

Personal data is any information relating to an identified or identifiable data subject. A data subject will 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 any other factor specific to the data subject's physical, physiological, economic, cultural or social identity.

A higher level of protection is awarded to all sensitive information. This includes personal data revealing nationality, racial or ethnic origin, political attitudes, trade union membership, religious and philosophical beliefs, prior criminal convictions, health status, sex life and genetic data of the data subject. Sensitive data also includes biometric data that permits direct identification or authentication of the data subject.

Restrictions on transfer of data offshore:

The free flow of personal data is not restricted if data is transferred to another European Union member state.

Personal data may be transferred to any other country if required by an international treaty, or if the personal data is transferred on the basis of a decision of an institution of the European Union or on the basis of a special approval granted by the Office for Personal Data Protection upon fulfilment of certain conditions specified in the Act.

Denmark

Danish data protection legislation is generally in line with the principles laid down in the EU Data Protection Directive 95/46 EC. However, stricter rules than required under this Directive have to some extent been adopted in Denmark. The data protection rules apply to both the public and the private sector and regulate the collection, processing and transfer of personal data as well as notification and authorisation requirements.

Applicable legislation:

The Danish Act on Processing of Personal Data, cf. Act no. 429 of 31 May 2000, as amended, (APPD) sets out the general rules applicable to data processing. In addition, special rules regarding data processing apply to certain activities/sectors e.g. the financial sector, the healthcare sector and the telecommunications sector.

The APPD applies to: (i) processing of data carried out on behalf of data controllers established in Denmark, if the activities are carried out within the territory of the European Economic Area; (ii) data controllers established in a third country if the processing of data is carried out using equipment placed in Denmark, unless such equipment is used only for the purpose of transmitting data through the territory of the EEA; and (iii) data controllers established in a third country if the collection of data in Denmark takes place solely for the purpose of processing in a third country.

Protected data:

The APPD regulates the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person (data subject). Personal data is divided into four categories which are subject to different processing rules:

(1) Ordinary personal data: Data not covered by the sections below;

(2) Semi-sensitive personal data: Data about criminal offences, serious social problems; and other purely private matters, other than those mentioned in section 3 below;

(3) Sensitive personal data: Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sex life; and

(4) Personal identification numbers: A data subject's social security number/personal identification number.

Processing of certain categories of personal data as well as processing for certain purposes requires both notification to and authorisation from the Danish Data Protection Agency.

Restrictions on transfer of data offshore:

Transfer of personal data to countries within the EEA is not specifically restricted.

Under the APPD, transfer of personal data to countries outside the EEA is prohibited unless one or more of the conditions below are met:

- the country in question ensures an adequate level of protection;
- the data subject has given his explicit consent;
- the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
- the transfer is necessary or legally required on 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 regulation 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 met 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;
- the transfer is necessary to safeguard public security, the defence of the Danish realm, or national security; or
- the Danish Data Protection Agency authorises the transfer based on (i) the EU Model Clauses, or (ii) Binding Corporate Rules.

In a number of instances, transfer of personal data to third countries is, in addition to the above, subject to both notification to and authorisation from the Danish Data Protection Agency.

Estonia

Estonia has implemented the system of data protection introduced by the EU Data Protection Directive 95/46 EC into national law. The adopted legislation lays down various principles of privacy and data protection rights for natural persons.

Applicable legislation:

Estonia has implemented the EU Data Protection Directive 95/46 EC through the Estonian Personal Data Protection Act 2007 (EPDPA). The EPDPA applies to both the public and private sector but is not applicable where personal data is processed by natural persons for personal purposes or where personal data is transmitted through Estonian territory without any other processing of the data in Estonia.

Data protection matters are also regulated by the Electronic Communications Act 2004, which implements the EU Directive on Privacy and Electronic Communications 02/58 EC.

There is also some relevant sector specific regulation in fields such as insurance and credit providers, security authorities and advertising.

The Estonian Data Protection Inspectorate has the power to issue monetary penalties of up to € 32,000 for non-compliance with the EPDPA.

Protected data:

Personal data under Estonian law is any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exists. Personal data for the purposes of Estonian law includes both digital and paper based records.

Sensitive data receives special protection. Sensitive personal data includes data on a person's political opinions, religious or philosophical beliefs, ethnic or racial origin, health records, genetic information, biometric data, sex life, trade union membership, criminal record or having fallen victim to an offence before relevant court procedures have taken place. Processors of sensitive personal data must register with the Estonian Data Protection Inspectorate or appoint a person responsible for processing personal data (a Data Protection Officer).

Restrictions on transfer of data offshore:

Principle
Transfer of personal data from Estonia is permitted only to a country which has a sufficient level of data protection.

EEA and White List
Members of the EEA and White Listed countries are deemed to provide a sufficient level of data protection. Data can therefore be transferred within these areas without restriction.

Safe Harbour
Personal data may also be transferred to US data importers with EU/US Safe Harbour certificates. This does not require the authorisation of the Estonian Data Protection Inspectorate.

Other countries
Data can be exported to a third country outside the EEA, the White Listed countries and organisations with US Safe Harbour certification if: i) the data subject explicitly consents to the transfer; or ii) the Estonian Data Protection Inspectorate authorises the transfer.

Authorisation is only granted by the Estonian Data Protection Inspectorate if the data controller ensures that the data subject's personal data is sufficiently protected. This can be achieved by including EU Model Clauses in a transfer agreement, which must be filed with the Estonian Data Protection Inspectorate along with a relevant application. Alternatively, a data controller can base the transfer to a third country on Binding Corporate Rules, with the authorisation of the Estonian Data Protection Inspectorate.

Finland

Finland has comprehensive and detailed legislation regarding the processing of personal data and personal data privacy. The legislation, which implements the EU Data Protection Directive 95/46 EC, applies to the automatic processing of personal data relating to a data subject (i.e. collecting, organising, processing, using, storing, deleting etc.).

Applicable legislation:

The Finnish Personal Data Act (enacted in 1999) (the Act) applies to both the public and the private sector in their respective automatic processing of personal data. The Act is not applicable to the processing of personal data by private individuals for purely personal purposes or otherwise comparable ordinary and private purposes.

The Act applies to a personal data controller subject to Finnish law (as based on the territoriality principle). The Act further applies to a controller who is not established in a Member State of the EU, but uses equipment located in Finland for processing personal data, except if the equipment is used solely for transferring data through the territory of Finland.

The processing of personal data requires legitimate grounds in law. The Act contains an exhaustive list of such legitimate grounds, out of which the most common ones are the data subject's explicit consent, or an underlying customer or other comparable relationship that justifies the processing.

The regulations of the Act are supplemented by, inter alia, the Act on the Protection of Privacy in Electronic Communications (which, for example, contains provisions on direct electronic marketing) and the Act on the Protection of Privacy in Working Life.

The Finnish Data Protection Ombudsman is vested with the primary powers to ensure compliance with the data protection framework, and also to issue guidance and preliminary opinions within the field.

Protected data:

Personal data is information concerning an individual, their qualities or living conditions that identifies the individual, their family or anybody living with them in the same household. The definition is broad and includes information concerning an individual's wealth income and information generated during a customer relationship with banks and credit institutions that constitutes, or is intended to constitute, a personal data file or a part thereof.

Higher restrictions apply to the processing of sensitive data, and such processing is primarily considered to be prohibited. Personal data is deemed to be sensitive when it relates to, or is intended to relate to, an individual's race or ethnic origin, political opinions, criminal record, sex preferences, health or need for social welfare services.

Restrictions on transfer of data offshore:

Personal data may be transferred outside the EEA only if the recipient country in question guarantees an adequate level of data protection. Finland observes the EC's decisions to approve certain countries outside the EEA as safe for data transfers. Data may be transferred to other third countries with the data subject's explicit consent, or if the data controller has entered into the EU Model Clauses.

The same rules for transfers also apply to outsourcing data processing activities, in as far as outsourcing is not considered under Finnish law as a transfer but as a use of a personal data file (by the help of a third party service provider). While transfers of personal data need only be notified under certain conditions, outsourcing data processing activities always triggers an obligation for both the data controller and the third party processor to make a notification to the Data Protection Ombudsman.

France

France has a comprehensive legislative regime arising from the implementation of the EU Data Protection Directive 95/46 EC.

Applicable legislation:

French Data Protection Act n°78-17 of 6 January 1978 (as amended) on data processing, data files and individual liberties (the French DPA).

The French DPA applies to the processing of personal data where the data controller: (i) carries out its activity on French territory within an establishment, whatever its legal form; or (ii) although not established in France or in the EU, uses means of processing located on French territory.

Depending on the nature of the data processed and/or of the purpose of the processing, personal data may not be processed under the French DPA without giving prior notice to, and/or, obtaining prior approval from, the Commission Nationale de l'Informatique et des Libertés (the CNIL).

The French DPA does not define the term "establishment" but the CNIL considers that there is an establishment where there is an effective and real exercise of an activity through stable arrangements. There is no clear definition of the concept of "stable arrangements" for instance, a branch may be considered by CNIL as an "establishment".

Protected data:

Under the French DPA:

- "personal data" is defined as "any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration".
- "processing of personal data" is widely defined as "any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction".

A higher degree of regulation applies to "sensitive information" relating to a person's race or ethnic origin, political opinions or association, religious or philosophical belief, trade union membership, sexual preference, criminal record, health or genetic information.

Non-compliance with the French DPA is subject to various administrative and criminal sanctions and, in particular, to a pecuniary sanction (pronounced by the CNIL) up to €150,000 and, if the breach occurs again within five years, up to €300,000 or, for legal entities, 5% of the turnover within the general limit of €300,000 and/or a criminal fine (pronounced by the Court) of up to €300,000 (€1.5 million for a corporate entity) and/or 5 years' imprisonment. Administrative and criminal sanctions are, in principle, cumulative. The CNIL and/or the Court may also order the publicity of the sanctions pronounced.

Restrictions on transfer of data offshore:

No restrictions on export to EEA countries or other White Listed (adequate data protection) countries.

Export to US entities covered by the EU/US Safe Harbour privacy regime is permitted.

Otherwise, transfer of data offshore is subject to restrictions (such as consent, EU Model Clauses or Binding Corporate Rules, CNIL's prior authorisation etc.).

Germany

Germany has detailed rules dealing with data protection, all consistent with and following the principles of the EU Data Protection Directive 95/46 EC. The data protection rules apply to both the public and the private sector and, in general, prohibit the collection, processing and use of personal data unless permitted by law or with the explicit consent of the person concerned.

Applicable legislation:

The "right to informational self-determination" is a constitutional right in Germany, protected by Art. 2 para. 1, and Art. 1 para. 1 of the German Grundgesetz (i.e. the German constitution).

Recently, the Federal Constitutional Court has held that this guarantee also comprises a fundamental right to the "confidentiality and integrity of IT systems".

Germany is said to be the jurisdiction that globally enacted the first data protection act ever in the year 1970. Currently, the main law for the protection of personal data is the Federal Data Protection Act 1990, as amended (major reforms were enacted in 2003 and 2009.) The Act generally applies to all businesses, irrespective of size and sector, that collect or process personal data.

Additional, sector specific data protection rules can be found in various other acts, such as the Telecommunications Act, the Telemedia Act (governing inter alia the use of data by internet websites), the Social Welfare Code and the German Energy Industry Act.

Special provisions apply to the public sector (in particular the Data Protection Acts of the German states – Länder).

Protected data:

The German data protection laws protect personal data of individuals that is collected, processed or used by a data controller that is subject to German data protection law. Personal data is any information concerning the personal or material circumstances of an identified or identifiable natural person. The data protection law provisions do not apply to anonymous data.

In rare cases, company data is also protected. According to the data protection law provisions of the Telecommunications Act, particulars of legal persons which are subject to the telecommunications secrecy obligation are treated as equivalent to personal data.

In accordance with the EU Data Protection Directive 95/46 EC, a higher degree of regulation applies to "special categories of personal data", i.e. information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership as well as health or sex life.

Furthermore, specific statutory secrecy obligations are enshrined in several laws, in particular the telecommunication secrecy obligation in Sec. 88 Telecommunications Act, as well as professional and official secrecy obligations (e.g. doctor patient confidentiality).

Restrictions on transfer of data offshore:

In Germany, there are two kinds of restrictions on a transfer of personal data. Firstly, as is the case for all EU Member States, the transfer of personal data to a recipient outside of the EEA is always subject to there being an adequate level of data protection in the offshore country. In the absence of an adequate level of data protection, transfers may exceptionally be made on the basis of Binding Corporate Rules, EU Model Clauses or other safeguards explicitly provided for in the Federal Data Protection Act.

Secondly, it must be borne in mind that, according to German data protection rules, any export of personal data outside of the EEA implies a transfer to a third party which generally requires justification (irrespective of where the recipient is located). In other words, the transfer to a third party requires to be justified in the first place. That means, it is required that either a statutory provision allows for the transfer or the data subject has consented.

According to German data protection laws, these restrictions to transfers of data to third parties even apply with regard to data transfers within a group of companies.

Gibraltar

Gibraltar is an overseas territory of the United Kingdom and, although part of the European Union, it is not a separate Member State. Gibraltar operates a data protection regime that is consistent with the EU Data Protection Directive 95/46 EC. There are some noticeable similarities between the data protection systems in Gibraltar and the United Kingdom.

Applicable legislation:

The United Kingdom delegates the implementation of directives in Gibraltar, to the local parliament but remains responsible to the European Union for such implementation. Gibraltar has implemented the EU Data Protection Directive 95/46 EC in the Data Protection Act 2004 (the Act).

The Data Protection Commissioner (the Commissioner) in Gibraltar regulates compliance with data protection law in the jurisdiction. The role is similar to that of the UK Information Commissioner.

The Commissioner can bring or defend legal actions in courts in Gibraltar and elsewhere and its powers include a power to apply for court ordered warrants. The Commissioner must co-operate with and assist supervisory authorities in states party to the Convention of June 1990 that applies the Schengen Agreement, by providing information on Gibraltar law and practice concerning data protection and automatic processing carried out in Gibraltar. The Commissioner has no duty to assist states outside the Schengen Agreement but is empowered to do so if he chooses.

Gibraltar has no data protection tribunal.

Protected data:

The Act applies to the processing of personal data, whether wholly or partly by automatic means and the non-automatic processing of personal data which forms, or is intended to form, part of a filing system.

Personal data is defined in the Act as meaning any information relating to a data subject, which is defined as a natural person who is the subject of personal data under the Act.

Processing of personal data is defined widely under the Act as any operation or a set of operations performed on personal data, by automatic or non-automatic means. Examples of processing include collecting, storing, recording, organising, consulting, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

A higher degree of protection applies to "sensitive personal data", which is defined as:

(a) data revealing racial or ethnic origin;

(b) data revealing political opinions;

(c) data revealing religious or philosophical beliefs;

(d) data revealing trade union membership;

(e) data concerning health or sex life;

(f) data concerning the commission or alleged commission of any offence by the data subject; and

(g) data concerning any proceedings for any 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.

The processing of sensitive personal data is generally prohibited, subject to a number of exceptions set out in the Act.

Restrictions on transfer of data offshore:

The data protection principles that apply to transfer of data offshore are the same as those applicable in the UK.

A data controller cannot transfer personal data to a country or territory outside Gibraltar unless the country is either a member of the EEA or adequately protects a data subject's personal data.

The adequacy of the level of protection is judged in all the circumstances of the case, with particular regard to a number of stipulated factors which include: the nature of the data, the destination country and its data protection scheme, the security measures that the importer will apply and the purposes for which the data is intended.

The general rules on the lawfulness of processing personal data also apply. Transfer is only permissible if the processing is fair (in practice this means that certain information must be made available to the data subject, including the purpose for which the data is to be processed) and at least one of the processing pre-conditions is satisfied. These include: the data subject's unambiguous consent to the processing and that the transfer is necessary for the performance of a contract to which the data subject is a party.

Exemptions that disapply the fair processing principle facilitate transfer of personal data abroad in certain contexts. These include an exemption for data processed for the purpose of "preventing, detecting or investigating offences", although it is generally believed that this is restricted to the data processing activities of enforcement agencies under a duty to prevent, detect or investigate offences. Compliance with the fair processing principle is not required to the extent that compliance prejudices that purpose.

There is a further exemption from the fair processing principle that applies where the personal data is required for the purposes of obtaining legal advice.

Greece

Greece has a comprehensive legislative framework regarding the protection of personal data, which is broadly in line with EU data protection legislation. The relevant provisions lay down the terms and conditions under which the processing of personal data is to be carried out so as to protect the fundamental rights and freedoms of individuals, and in particular, their right to privacy.

The Hellenic Data Protection Authority (the HDPA) is an independent authority, with regulatory, administrative and audit competencies, to safeguard compliance with Greek data protection legislation.

Applicable legislation:

Data protection is a fundamental right of individuals under the Greek Constitution (article 9A).

The main law for the protection of personal data is Law 2472/1997, which transposed the EU Data Protection Directive 95/46 EC into Greek law. Further, Law 3471/2006 (regarding the protection of personal data and privacy in the electronic communications sector) implemented the European Directive Privacy and Electronic Communications 02/58EC. Law 3873/2009, in the telecommunications sector, sets the framework for the disclosure of users' data for national security and criminal investigation purposes.

Moreover, Law 3917/2011 (regarding the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks) implemented European Directive 24/2006 and inserted new provisions regarding the use of video surveillance systems for the protection of goods and persons.

In addition, a few Directives and Regulations of the HDPA are also in place, with respect to data protection in the banking, public administration, insurance, health and tax sectors.

According to the provisions of Law 3943/31.3.2011 and Ministerial Circular 1185/1.9.2011, the personal data of persons whose unpaid debts to the Greek State exceed €150,000 will be made publicly available on the internet. The disclosed data will include, among others, the names, VAT numbers and the amount of debt of the tax defaulters. The HDPA has delivered opinion no. 4/14.10.2011, in which it is stated that the aforementioned provisions for the disclosure of personal data are justified and acceptable, in terms of the purpose pursued.

Law 4170/2013 facilitates access by public authorities which exercise duties tax collection, tax evasion control and financial crime duties, to taxpayers' bank accounts. Access is now available through a web platform administered by the General Secretariat for Information Systems of the Ministry of Finance. The details of the operation of the platform are provided by the Ministerial Circular 1258/6.12.2013. The HDPA has delivered its opinion no. 5/2013, in which it included its comments on the operation of the platform.

Protected data:

Any information relating to the data subject is protected under the provisions of the prevailing Greek legislation (e.g. name, age, address, profession, marital situation, education, financial status etc.).

Restrictions on transfer of data offshore:

No restrictions apply with respect to the transfer of data within the EU or to White Listed countries. However, a relevant notification must be filed with the HDPA prior to the transfer.

Upon authorisation by the HDPA, personal data may be transferred to other countries, provided that they guarantee an adequate level of protection. Transfer of data to countries which do not guarantee adequate protection may be permitted by way of exception if the HDPA authorities the transfer and one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the protection of vital contracts, and/or the transfer is required for reason of public interest. The transfer of data to countries which do not guarantee adequate protection may be permitted only by way of exception, subject to authorisation by the HDPA and provided that additional requirements are met (such as consent of the data subject, necessity of the transfer for the protection of vital interests, or for reasons of public interest, or for the establishment, exercise or defence of a right in court etc.).

Specifically for the EU/US, transfer of data is permitted on the condition that the recipient company is covered by the US Safe Harbour privacy regime.

Hungary

Hungary has rules on data protection consistent with the applicable EU Data Protection Directive 95/46 EC.

Applicable legislation:

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Act). Hungarian data protection legislation is primarily based on the newly promulgated Fundamental Act of Hungary (25 April 2011), where article VI (2) provides that everyone has the right to the protection of his/her personal data as well as to have access to and disseminate information of public interest. Therefore, the Fundamental Act of Hungary regards the protection of personal data as a fundamental right of the individual.

Protected data:

Under the Act personal data means any information relating to an identified or identifiable natural person (private individual) and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information shall be treated as personal data as long as the data subject remains identifiable throughout the processing. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to his/her name, to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Personal data may be processed if the private individual has given his/her consent, or if decreed by law or by a local authority based on authorisation conferred by law concerning specific data defined therein. However, "special data" may only be processed if the data subject has given his explicit consent in writing, or prescribed by treaty concerning the personal data if ordered by law in connection with the enforcement of some constitutional right, for national security or law enforcement purposes or, finally, if ordered by law in other cases.

Where it serves the public interest, free access to particular personal data may be ordered by law. In all other cases, free access to personal data may be provided only with the consent of the data subject, (such consent must be in writing in the case of special data). If there is any doubt, it is presumed that the data subject did not consent to allow free access.

Restrictions on transfer of data offshore:

Transfer of personal data within the European Economic Area member states is free of all restrictions and is treated as if the transmission took place within the territory of Hungary.

Personal data may be transferred to a non-EEA third country controller or data processor if the data subject has given his/her express consent or the transfer is permitted by law and the laws of the third country in question afford an adequate level of protection with respect to the processing of the personal data transferred. Data protection is regarded as adequate if: (i) the EU Commission has determined that the third country in question ensures an adequate level of protection (the country is White Listed); or (ii) there is a bilateral treaty between the third country and Hungary containing guarantees for the rights of data subjects; or (iii) the third country controller or processor offers appropriate safeguards to ensure an adequate level of protection, such as EU Model Clauses.

Removed restrictions on sub-processing:

According to an amendment to the provisions of the Act affecting sub-processing arrangements, (effective from 1 July 2013) the data processor is allowed to engage additional data processors (sub-processors) in accordance with the instructions of the data controller. The data controller is able to allow the data processor to engage sub-processors and to define the conditions of their involvement.

Changed liability rules:

As of 15 March 2014, the liability provisions of the Act changed in line with the new Civil Code of Hungary. Under the previous rules the data controller was liable for any damage caused to a data subject as a result of unlawful processing or by any breach of data security requirements. A new provision now affords a data subject the right to claim restitution (i.e. called injury fee) from the data controller where the data subject's personality rights have been violated as a result of unlawful processing of their data or by any breach of data security requirements. The data controller may be exempted from liability for damages and payment of restitution if he proves that the damage or the violation of personality rights were caused by reasons beyond the data controlling activities and beyond his control.

Iceland

Iceland has a legislative regime that implements the EU Data Protection Directive 95/46 EC.

Applicable legislation:

Iceland has implemented Directive 95/46 EC through Act No 77/2000 on the Protection and Processing of Personal Data Protection Act (the Data Protection Act). This is the key piece of data protection legislation in Iceland.

The Icelandic Data Protection Authority is responsible for the enforcement of the Data Protection Act. Infringements of the Data Protection Act, and of regulations issued according to it, are punishable by means of fines or a prison term of up to three years, unless more severe sanctions are provided for in other acts of law.

Protected data:

Personal data is any data relating to the data subject (identified or identifiable), i.e. information that can be traced directly or indirectly to a specific individual, deceased or living.

Sensitive personal data means information in respect of: the data subject's origin, skin colour, race, political opinions, religious beliefs and other life philosophies; whether a person has been suspected of, indicted for, prosecuted for or convicted of a punishable offence; the data subject's health data, including genetic data and data on the use of alcohol, medical drugs and narcotics; the data subject's sex life (and sex behaviour); and trade union membership.

Restrictions on transfer of data offshore:

Principle

The transfer of personal data to another country is permitted if the laws of that country provide an adequate level of personal data protection.

EEA, White List and Safe Harbour

Countries of the European Economic Area, White Listed countries and organisations that comply with the EU/US Safe Harbour program are deemed to provide sufficient data protection and transfers to these places do not require approval.

Other countries

The transfer of personal data to a country that does not provide an adequate level of personal data protection is prohibited, unless an exemption applies. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest. Where an exemption applies, the Icelandic Data Protection Authority's approval is not required.

The Icelandic Data Protection Authority can also authorise a transfer of personal data to a third country that inadequately protects data if the data controller demonstrates that adequate safeguards have been put in place to protect the rights of the data subject. A common solution is to use EU Model Clauses in the transfer agreement with the recipient of the data. This solution still requires the Icelandic Data Protection Authority's approval.

Ireland

Ireland has a comprehensive legislative regime that implements the EU Data Protection Directive 95/46 EC. It regulates how a data user (i.e. a data controller or data processor) should collect, hold, process, disclose or use personal data relating to a data subject.

Applicable legislation:

Data protection in Ireland is governed by the Data Protection Acts 1988 and 2003 (together, the DPA) which sets out the law relating to data protection generally, and by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 which sets out the law relating to data protection and privacy in the context of electronic communications networks and services generally.

Protected data:

The DPA regulates the collection, processing, keeping, use and disclosure of personal data.

Personal data is data relating to living individuals (referred to in the DPA as "data subjects") who are or can be identified from the data or from the data together with other information that is in, or is likely to come into, the possession of a person who controls the contents and use of the personal data (the "data controller").

Restrictions on transfer of data offshore:

Under the DPA, transfers of personal data to countries outside the EEA are prohibited unless either:

- the destination country in question ensures an adequate level of protection for the processing of personal data; or
- one or more pre-conditions are satisfied thereby allowing the transfer to take place.

Examples of pre-conditions include:

- where 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
- the rights of the data subject are protected by a contract based on the EU Model Clauses for the transfer of personal data to countries outside the EEA which has been entered into between the sender and the recipient of the personal data.

If a destination country has not been approved by the European Commission as having "adequate" level of protection (or, if the business receiving the personal data is in the US and it has not signed up to the EU/US Safe Harbour principles) then it is advisable to make sure that the transfer meets one of the transfer pre-conditions, rather than to rely on a self-assessment of the adequacy of the measures in place.

Italy

Italy has a comprehensive legislative regime that implements the EU Data Protection Directive 95/46 EC.

Applicable legislation:

The Privacy Code 2003 (Legislative Decree n. 196 of 30 June 2003) (the Code) The Code consolidated previous pieces of legislation, implementing EU Data Protection Directive 95/46 EC of 24 October 1995 and n. 02/58 EC of 12 July 2002 on data protection.

Since its enactment, the Code has been amended several times. Today, the Code provides a general system of data protection for natural persons, with specific reference to sensitive data, under the guidance, supervision and (to some extent) jurisdiction of a National Authority.

Protected data:

Protected data, as defined in the Code is "any information relevant to a natural person, that is identified or identifiable, directly or indirectly, through any other information, including a personal identification number". Protection is therefore granted only to natural persons unless data is treated on an anonymous basis. Corporations and entities enjoy limited protection, consisting of their right to register with the Italian Register of Oppositions to unsolicited marketing communications by telephone or mail.

Restrictions on transfer of data offshore:

Transfer within the European Union is not restricted.

Transfer outside the European Union is permitted, if one or more of certain conditions are met, namely:

(1) that the data subject expressly agreed to the transfer;

(2) that transfer is necessary to perform a contract to which the data subject is a party;

(3) that transfer is necessary for reasons of a substantial public interest;

(4) that transfer is necessary for vital medical reasons;

(5) that transfer is necessary to allow personal investigations in a criminal case;

(6) that transfer is related to data contained in a public database;

(7) that transfer is justified by a limited number of study purposes;

(8) that, upon request of the transferor, the transfer is allowed by the National Authority, if they have checked that effective data protection is provided by a suitable contract between transferor and transferee or, if data are transferred within the same group of companies, if they have checked that applicable group policies guarantee an effective data protection. In the first case, the use in the contract of EU Model Clauses, without any amendment to the same, exempts the transferor from seeking permission from the National Authority; or

(9) that transfer is allowed by the National Authority, on the basis of the EU/US Safe Harbour privacy regime.

Kazakhstan

Until 2013, Kazakhstan did not have a specific regulatory framework for data protection. On 21 May 2013 the Parliament of Kazakhstan adopted Law "On Personal Data And Their Protection" № 94-V (the Data Protection Law), which came into force on 25 November 2013. The Data Protection Law introduced the concept of personal data and defined the permitted use of personal data. Additionally, if introduced principles of organisational and legal support of activities for legal entities and state agencies, organising and carrying out the processing of personal data.

Applicable legislation:

The Data Protection Law

The Data Protection Law defines the purpose, principles and legal framework that govern the collection, processing and protection of personal data.

The purpose of the Data Protection Law is to ensure the protection of the rights and freedom of individuals in the collection and processing of their personal data by any data controller or data processor.

Generally, the collection, processing and protection of personal data shall be carried out in accordance with the principles of:

(1) compliance with the constitutional rights and freedoms of the individual;

(2) the rule of law;

(3) the confidentiality of personal data to which access is limited; and

(4) the maintenance of the security of individuals, society and the state.

In addition to the Data Protection Law, there is general legislation which also provides for the protection of the right to privacy of an individual's personal data. In particular, the Constitution, the Law on the Informatisation, the Civil Code, the Code on Health of the People and the Health System and the Labour Code provide certain provisions that regulate the protection and transmission of personal data. Below, we briefly outline these provisions of legislation.

The Constitution

Article 18 of the Constitution guarantees the privacy of an individual's personal life, bank accounts, correspondence, telephone conversations, postal and other messages. However, there are no statutory provisions or case law which define the scope of the above constitutional provision.

The Law on Informatisation

According to the Law on Informatisation dated 11 January 2007, personal data is information about facts, events, life circumstances of an individual and/or data enabling identification of an individual. Electronic information resources that contain personal data, must maintain the privacy of personal data from the moment of collection until its destruction, depersonalisation or until obtaining the consent to its disclosure from the person to whom the data relates. Receiving, processing and use of such data is limited to the purposes for which they are collected. Subsequent transfer of electronic information resources that contain personal data is permitted only with the consent of the person to whom the data relates, except where provided for by legislation of Kazakhstan. Furthermore, nobody has the right to demand from individuals details about their private lives which consist of personal and family privacy, secrecy of correspondence, telephone conversations, postal, telegraphic and other communications of individuals, including information relating to their origin, health, beliefs, political or religious beliefs, or to receive such information for the development of electronic information resources without their consent.

The Civil Code

Under the Civil Code dated 27 December 1994, a citizen has the right to protection of personal privacy, including secrecy of correspondence, telephone conversations, diaries, notes, memos, intimate life, adoption, birth, medical, advocacy and bank accounts. The publication of diaries, notes, memos and other documents shall be allowed only with the consent of the author. The publication of letters shall only be allowed with the consent of the author and the addressee. In the event of the death of any of them, these documents may be published upon obtaining consent of the survived spouse and children of the deceased.

The Code on Health of the People and the Health System

Under the Code on Health of the People and the Health System dated 18 September 2009, reporting on the health status of patients for the development of electronic information resources can be carried out only with the consent of the patient. Access by medical personnel to electronic information resources that contain personal medical records of patients should be restricted only for the purposes of providing medical care.

The Labour Code

According to the Labour Code dated 15 May 2007, an employee's "personal information" is information about the relevant employee collected during their employment. The employer must not disclose personal information of any employee to third parties without the relevant employee's written consent. The access to personal data of employees can be given only to the authorised officers of the employer required to perform their job functions.

Protected data:

The Data Protection Law defines "personal data", as "data related to a specific individual or an individual who may be identified on the basis thereof and which is fixed on electronic, paper and/or other material objects." Such personal data may include a person's name, ethnic group or nationality, gender, date and place of birth, individual identification and registration numbers, address and contact details, marital and family status, data related to the ownership of property, education, profession, religion, medical and biometrical data.

Restrictions on transfer of data offshore:

According to the Data Protection Law, the transfer of personal data to a foreign state can be carried out only if that state ensures the due protection of personal data either pursuant to its national laws and regulations or under relevant international treaties, for example, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. Transfer of personal data to foreign countries can be prohibited or restricted in cases when such restriction or prohibition is required in order to protect the constitutional order of Kazakhstan, health rights and lawful human interests, national defence and national security.

Latvia

Latvia has comprehensive data protection legislation, which implements the EU Data Protection Directive 95/46 EC. This legislation applies to both public and private entities, and regulates the terms, conditions and circumstances under which personal data may be collected, processed, stored and used.

Applicable legislation:

Latvia has implemented the EU Data Protection Directive 95/46 EC through the Personal Data Protection Law 2000 (the Personal Data Protection Law) and the EU Directive on Privacy and Electronic Communications 02/58 EC through the Law on Electronic Communications 2004.

There are also specific rules applicable to electronic documents, biometric data, medical services, debt collection services, e-commerce and the telecommunications sector, which provide stronger protection for human data subjects in these fields.

The State Data Inspectorate enforces the data protection legislation in Latvia. The State Data Inspectorate has the power to issue monetary penalties of up to €14,000 in misdemeanour proceedings for non-compliance with the Personal Data Protection Law.

Protected data:

Personal data is defined as any information relating to an identified or identifiable natural person. Sensitive personal data is defined as data that reveals the race, ethnic origin, religious or philosophical beliefs, political convictions, trade union membership or information concerning the health or sex life of a person.

Restrictions on transfer of data offshore:

Principle

Personal data may be transferred to another state if that state ensures the same level of data protection as Latvia.

EEA, White List and Safe Harbour

There are no restrictions on data transfers inside the European Economic Area, to White Listed countries and to companies participating in the EU/US Safe Harbour system.

Other countries

Data can be exported to other jurisdictions if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest.

Moreover, the data controller must undertake to supervise that all applicable data protection measures are fulfilled, by entering into a written data transfer agreement with the recipient of personal data. Provisions to include in the contract are established by the Latvian Counsel of Ministers and the use of EU Model Clauses is recommended. Another way to achieve a compliant export is by use of the Binding Corporate Rules.

Prior to any transfer of personal data outside the EEA, the relevant data processing activities must be registered with State Data Inspectorate, unless the data controller is exempt from registration.

Lithuania

The Lithuanian data protection regime complies with the EU Data Protection Directive 95/46 EC.

Applicable legislation:

Lithuania has implemented the EU Data Protection Directive 95/46 EC with the Law on Legal Protection of Personal Data 1996, which has been amended several times. This is the key piece of data protection legislation in Lithuania and applies to both public and private entities that process personal data.

Rules applicable to personal data protection are also found in other pieces of legislation, including:

(1) The Law on Electronic Communications 2004, as amended. This implements the EU Directive on Privacy and Electronic Communications 02/58 EC.

(2) The Law on Provision of Information to the Public 1996, as amended.

The Lithuanian State Data Protection Inspectorate enforces the personal data protection laws.

Under the Lithuanian Administrative Code, non-compliance is sanctioned by a relatively small fine (up to €290) for the first infringement, however a fine for a second infringement is up to €580.

Protected data:

Personal data is defined as any information relating to a natural person (the data subject), who can be identified, directly or indirectly, from that data. Personal data includes: a personal identification number and information concerning a person's physical, physiological, mental, economic, cultural or social condition.

Greater protection is accorded to sensitive personal data. This consists of information on a person's racial or ethnic origin, political religious, philosophical or other beliefs, trade union membership, health, sex life and criminal convictions.

Restrictions on transfer of data offshore:

Principle
Data can only be transferred to third countries that guarantee an adequate level of data protection.

EEA and White List
There are no restrictions on the transfer of data within the European Economic Area. Transfers to White Listed countries are permitted, but are subject to the approval of the Lithuanian State Data Protection Inspectorate.

Other countries
Data can be exported outside the EEA without prior authorisation if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest.

If none of these conditions are met, export outside the EEA depends on the authorisation of the Lithuanian State Data Protection Inspectorate. Authorisation is granted where the State Data Protection Inspectorate considers that the destination country provides an adequate level of protection.

Authorisation may also be granted where the destination country lacks sufficient data protection rules, if the data exporter/data controller adopts measures to adequately protect the personal data within the transfer agreement or other written document with the data recipient.

This can be achieved by using Binding Corporate Rules, EU Model Clauses or making a transfer on the basis of the EU/US Safe Harbour system. Even where a data exporter puts in place these protective measures, authorisation from the State Data Protection Inspectorate is still required to export the data.

Luxembourg

Luxembourg's data protection rules are compliant with the principles as laid down in the EU Data Protection Directive 95/46 EC. The competent authority for the supervision of proper application of data protection rules in Luxembourg is the National Commission for the Protection of Data (Commission Nationale pour la Protection des Données (CNPD)). The implemented Directive protects the fundamental rights of natural persons.

Applicable legislation:

Directive 95/46 EC on data protection has been implemented in Luxembourg through a Law of August 2, 2002 on the Protection of Persons with regard to the Processing of Personal Data, as modified by a Law of July 28, 2011 (the Data Protection Act).

Furthermore, the EU Directive on Privacy and Electronic Communications 02/58 EC has been implemented in Luxembourg through the Law of May 30, 2005, as modified by a Law of July 28, 2011. The Law lays down specific provisions for the protection of persons regarding the processing of personal data in the electronic communications sector.

Protected data:

The Data Protection Act defines "protected data" as any information of any type, including sound and image, relating to an identified or identifiable natural person.

Furthermore, the Data Protection Act grants special protection to sensitive data such as: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health or sex preference, including the processing of genetic data.

Restrictions on transfer of data offshore:

Subject to other more specific legislation applicable to some economic sectors, data can be transferred within the EEA without any restriction but each transfer of data needs to be notified to the CNPD beforehand. Prior to the transfer of sensitive data, a written authorisation of the CNPD is required.

As a matter of principle, data cannot be transferred outside of the EEA, except if the in-sourcing country ensures equivalent data treatment to Luxembourg and if the level of protection is in accordance with the Luxembourg level of protection.

Transfer of data to a third country outside of the EEA is possible without restriction in limited circumstances where the data subject specifically consents to such transfer.

Malta

Malta has implemented and transposed the provisions of the EU Data Protection Directive 95/46 EC and other related EU Directives through a number of pieces of primary and subsidiary legislation. The local authority responsible for data protection is the Office of the Information and Data Protection Commissioner (the Commissioner's Office).

Applicable legislation:

Malta has implemented EU Directive 95/46 EC through the Data Protection Act 2001 (Chapter 440 of the Laws of Malta) (the Act). The provisions of Directives 02/58 EC, 06/24 EC and 09/136 EC have been implemented through a number of local regulations. The Commissioner's Office has also promulgated various other regulations, including those that specifically concern the processing of personal data relating to minors and the processing of personal data by the police. A number of sector specific guidelines, including personal data processing in education, insurance, banking, credit referencing, CCTV and biometrics have also been published.

The Act applies to the processing of personal data (including sensitive personal data), whether wholly or partly by automated means and to non-automated processing where the personal data forms or is intended to form part of a filing system.

The Commissioner's Office has the authority to issue fines or other penalties up to a maximum of €23,300 and can in certain cases also request the courts to impose imprisonment terms of not more than six months.

Protected data:

The Act regulates the processing of "personal data" and "sensitive personal data" by data controllers. "Personal data" is defined 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. "Sensitive personal data" is defined as personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life.

Restrictions on transfer of data offshore:

Basic Principle

A transfer of personal data to another country constitutes processing and as such must be notified to the Commissioner's Office in the same way as other processing operations.

EEA, White List and Safe Harbour

No restrictions or other formalities (beyond notification) apply to the transfer of personal data to EU Member States, EEA countries, White Listed countries and EU/US Safe Harbour certified organisations.

Other countries

Data can be exported to other third countries with the approval of the Commissioner's Office. The Commissioner's Office will only approve the transfer where the data controller has provided adequate safeguards, particularly by means of appropriate contractual provisions such as EU Model Clauses.

Data can be exported to jurisdictions that do not ensure an adequate level of protection without the approval of the Commissioner's Office, if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest. Even though approval is not required to export where one or more of these conditions are met, the data controller would still need to notify the Commissioner's Office of the transfer.

The Netherlands

The Netherlands has a comprehensive and developed data protection law that covers both public and private sectors in society.

Applicable legislation:

The Netherlands implemented the EU Data Protection Directive 95/46 EC by means of: (i) the Act on the Protection of Personal Data of 6 July 2000 (the DPA); and (ii) the Exemption Decree DPA of 7 May 2001 (the Decree).

The DPA regulates the protection of individuals with regard to the processing of personal data by data controllers and data processors, amongst other things, by imposing an obligation to provide fair processing of information. In addition, data controllers and data processors have to notify the Dutch Data Protection Authority (College bescherming persoonsgegevens) about the fully, or partly, automated processing of personal data before such processing may begin.

Pursuant to the Decree, certain categories of processing are exempt from the obligation to notify, such as the processing of certain data as part of personnel administration. In general, the exemptions as described in the Decree do not apply to the transfer of personal data to countries outside of the EEA that do not offer an adequate level of protection.

Protected data:

The DPA protects personal data which is defined as any information relating to an identified or identifiable individual. An identifiable individual is someone who can be identified, directly or indirectly, in particular by reference to information which, by itself or in combination with other information, can be linked to his or her identity.

Restrictions on transfer of data offshore:

There are no restrictions on the transfer of personal data to EEA countries or to White Listed countries. The transfer of personal data to countries outside of the EEA which are not White Listed is allowed only, for instance, with the unambiguous consent of the data subject, by entering into EU Model Clauses or with a permit from the Dutch Minister of Justice.

Norway

Norway has a comprehensive legislative regime that implements the EU Data Protection Directive 95/46 EC.

Applicable legislation:

The Act on Processing of Personal Data dated 14 April 2000, as last amended 11 January 2013, and the supplementary Regulation on Processing of Personal Data dated 15 December 2000, as last amended on 19 August 2013, implement the EU Data Protection Directive 95/46 EC.

Protected data:

Personal data is to be understood as any information and assessments which may be linked to a natural person, either on a stand-alone basis or in conjunction with other information.

Personal data primarily covers digital information but extends to some structured paper based records where the organisation of the information also allows the searcher to find different categories of information about the individual without further analysis.

A higher level of protection is given to all "sensitive information". This includes personal data revealing nationality, racial or ethnic origin, political attitudes, trade union membership, religious and philosophical beliefs, prior criminal convictions, health status and sex orientation.

Restrictions on transfer of data offshore:

The EU Data Protection Directive 95/46 EC grounds allowing transfer outside of the EEA or White Listed countries have been implemented, such as where the data subject has consented or where the processing is necessary to perform a contract with the data subject. Otherwise, transferring on the basis of EU Model Clauses or the EU/US Safe Harbour certification system provides the most straightforward route to achieve compliant export.

Poland

Poland has a set of data privacy principles which are consistent with the principles in the EU Data Protection Directive 95/46 EC. These principles apply to governmental bodies and the private sector.

Applicable legislation:

Act dated 29 August 1997 on personal data protection (Journal of laws of 2002, no. 101, item 926, as amended) (the Personal Data Protection Act)

The Personal Data Protection Act implements the EU Data Protection Directive 95/46 EC. It provides for a general system of personal data protection and criminal, as well as civil liability, for non-compliance.

There are also industry specific rules for banking, insurance, medical services, e-commerce and telecommunications which exclude the application of the Personal Data Protection Act to the extent they provide for stronger protection.

Protected data:

Personal data is defined as all information relating to an identified or identifiable individual.

An identifiable individual is a natural person whose identity may be determined, directly or indirectly, in particular by reference to his/her identification number or one or more specific factors relating to his/her physical appearance or physiological, mental, economical, cultural or social features. Information is not regarded as enabling a person to be identified if such identification would require excessive costs, time or activity.

A higher degree of regulation applies to "sensitive information" relating to, inter alia, a person's race, ethnic origin, political opinions or association, religious or philosophical belief, union membership, sex preference, criminal record, health or genetic information.

Processing of such information is generally prohibited, subject to limited exceptions.

Restrictions on transfer of data offshore:

Transfer within the European Economic Area is not restricted. Transfer to countries outside of the EEA is only permitted if at least one of the following conditions is met:

(1) consent of the interested person has been obtained;

(2) transfer of data to a third country is necessary to perform an agreement made between the interested person and the data administrator or in favour of the interested person;

(3) transfer is necessary for public good or for purposes of evidencing claims;

(4) transfer is necessary for purposes of the vital interests of the interested person's protection; or

(5) data is publicly available.

Portugal

Portugal has a comprehensive legislative regime that implements the EU Data Protection Directive 95/46 EC.

Applicable legislation:

In 1998 Portugal issued Act 67/98 transposing Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 (Act 67/98), on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Portuguese Constitution also establishes the general data protection principles, and other specific laws, such as labour and electronic communications laws, include specific data protection rules.

In addition, the Data Protection Authority issues guidelines and recommendations, setting out specific rules and procedures for data processing.

Protected data:

According to Act 67/98, "personal data" means any information of any type, irrespective of the medium involved, including sound and image, relating to an identified or identifiable natural person (data subject). 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.

This definition is wide enough to encompass, for example, video surveillance, policies for using e-mails, internet and phone calls at the workplace and whistleblowing hotlines.

Restrictions on transfer of data offshore:

Without prejudice to the need to register data transfers, personal data may move freely between member states of the European Union.

Regarding data transfers outside the member states, they may be subject to an authorisation or a mere notification, depending on the particular circumstances. Specifically, a notification must be filed whenever transfers are executed by means of the EU Model Clauses, or if some specific legal requirements are met.

Romania

Romania has a legislative regime that implements the EU Data Protection Directive 95/46 EC.

Applicable legislation:

Romania has implemented the EU Data Protection Directive 95/46 EC through Law no. 677/2001. The EU Directive on Privacy and Electronic Communications 02/58 EC has also been implemented in Romania, with two pieces of legislation. These are: i) Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector; and ii) Law no. 298/2008 on the retention of data generated or processed on publicly available electronic communications, services or public communications networks.

The National Supervisory Authority For Personal Data Processing has powers to issue fines of up to RON 50,000 (approx. €11,000) for non-compliance with the Law no. 677/2001 on data protection.

Protected data:

Personal data is any data from which a living individual (the Data Subject) may be directly or indirectly identified, by reference to an identification number or to one or more factors specific to the Data Subject's physical, physiological, mental, economic, social and cultural identity, by any private or public entity or individual that performs operations with regard to personal data by automatic or non-automatic means (the Data Controller).

The processing of personal data covers any type of data management, including: collection, recording, organisation, storage, adjustment or amendment, extraction, consultancy, use, disclosure to third parties, annexation, combination, blocking, deletion or destruction.

Sensitive personal data is subject to greater levels of protection. Sensitive personal data includes information concerning: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union or political membership, health or sex life, genetic or biometric data, criminal convictions or security measures, personality aspects, professional competence, credibility and behaviour, solvency and economic or financial position, personal identification number (CNP) and any data of children under 18 years old.

Restrictions on transfer of data offshore:

Principle

Any transfer of personal data to any state requires prior notification to the National Supervisory Authority For Personal Data Processing (NSAPDP). Any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.

EEA, White List and Safe Harbour

Transfer of data to countries within the EEA and to White Listed countries is permitted without authorisation, but the NSAPDP must be notified of the export. A transfer can also be made on the basis of the EU/US Safe Harbour certification system, provided that the receiving party presents a valid certificate and the NSAPDP is notified.

Other countries

Data can be exported to other jurisdictions not deemed to provide sufficient data protection if one or more of a number of specified conditions is met. These include that the Data Subject explicitly consents, the transfer is necessary for the performance of a contract for the Data Subject and the transfer is necessary to serve an important public interest. Even where a condition is satisfied, the NSAPDP must approve the transfer.

EU Model Clauses can also be used to achieve a compliant export to third countries, with the approval of the NSAPDP.

Russia

Russia's Personal Data Law regulates the processing of personal data by public bodies and private entities.

Applicable legislation:

In general, in Russia protection of personal data is subject to regulation by the Federal Law No. 152-FZ of 27 July 2006 "On Personal Data" (the Personal Data Law).

The Personal Data Law regulates the processing of personal data by federal, regional and local authorities, legal entities and individuals (i.e. Personal Data Operators).

Protected data:

The Personal Data Law defines the concept of "personal data" as any information concerning a certain individual or an individual that may be identified on the basis of that information (the Data Subject), including his or her family name, first name, patronymic, the year, month, date and place of birth, address, family, social or property status, education, profession, income and other information.

The Personal Data Law introduces special categories of personal data (i.e. related to race, nationality, political views, religious or philosophical beliefs, health and private life of a Data Subject) which shall not be processed except in cases directly stipulated in the Personal Data Law.

The Personal Data Law contains a general requirement that personal data processing shall be allowed only with the consent of the Data Subject. However, the Personal Data Law contains a short exhaustive list of cases when consent of the Data Subject is not required.

The Personal Data Law also determines the main obligations of Personal Data Operators. A Personal Data Operator shall: provide the Data Subject with information related to processing of its personal data; grant a Data Subject access to its personal data; ensure safety of personal data processing; change, delete or block personal data upon the demand of a Data Subject; and in cases stipulated by the law, notify an authorised body for the protection of the rights of Data Subjects of its intention to perform personal data processing.

Restrictions on transfer of data offshore:

The Personal Data Law introduces a procedure for the transfer of personal data by a Personal Data Operator across the Russian state border to a foreign public authority, individual or legal entity.

The transfer of data outside of Russia does not require additional consent from the Data Subject if the jurisdiction that the personal data is transferred to also ensures adequate protection of personal data. In particular, the Personal Data Law allows such transfer of personal data to countries outside Russia that are parties to Convention 108. The Personal Data Law also authorises the Russian Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roscomnadzor) to approve a list of foreign countries that are not parties to Convention 108 but guarantee adequate protection of rights of Data Subjects.

However, the transfer of data to a territory that does not ensure adequate protection of the rights of Data Subjects is permitted only in cases directly stipulated by the Personal Data Law, for example, subject to written consent of the Data Subject or for the purpose of performance of an agreement to which it is a party.

Serbia

Although Serbia is not a member of the EU and so has not systematically implemented the EU Directives, the Serbian data protection regime reflects the basic principles of the EU Data Protection Directive 95/46 EC.

Applicable legislation:

The Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti, Official Gazette of the Republic of Serbia nos. 97/2008, 104/2009, 68/2012, and 107/2012) (the Law), together with related bylaws, sets out the rules that apply to the collection and processing of personal data in Serbia. It applies to entities in both the public and private sector.

The Commissioner for Information of Public Importance and Personal Data Protection (the Commissioner) enforces the Law. Non-compliance with the obligations set out by the Law constitutes a misdemeanour, for which the data controller or data processor in breach may be fined up to RSD 1,000,000 (approx. €8,600).

Other laws relevant to the field of data protection and privacy include the Law on Consumer Protection (2010) and the Law on Electronic Trade (2009), which protect against unsolicited communications.

Protected data:

The Law regulates the processing of personal data. Personal data means any information relating to an individual regardless of the form of its presentation or any other characteristic of such information. "Individual" means any data subject who is or can be identified on the basis of his/her name, unique personal identification number, address or any other distinguishing feature of his/her physical, psychological, spiritual, economic, cultural or social identity.

Processing is widely defined as any operation undertaken in relation to personal data (e.g. collection, classification, recording, use, storage, etc.).

Special protection is granted to sensitive personal data. This includes information concerning a person's: nationality, race, gender (in practice, the Commissioner treats data on mere gender as non-sensitive data and regards only data on transgender or transsex traits as sensitive), language, religious beliefs, membership of a political party or trade union, health, receipt of state benefits, status as a victim of violence, criminal convictions, and sex life.

Restrictions on transfer of data offshore:

Transfer of personal data from Serbia to a country which is a party to Convention 108 does not require approval from the Commissioner. However, transfer of personal data to any country which is not a party to Convention 108 must be pre-approved by the Commissioner.

The Commissioner's pre-approval is required to transfer personal data to the United States, regardless of whether the recipient company is EU/US Safe Harbour certified or not.

When deciding whether to authorise a request to transfer personal data abroad, the Commissioner considers whether the laws of the destination country and/or the data transfer agreement ensure a level of personal data protection comparable to that provided by Convention 108.

Slovak Republic

The Slovak Republic has implemented the EU Data Protection Directive 95/46 EC. It has recently adopted new legislation, effective from 1 July 2013, following reform of the EU legal framework and the recommendations of the Schengen Evaluation, which clarifies the applicable law, more precisely defines terms and sets out more clearly the necessary processes.

Applicable legislation:

The Slovak Republic has implemented the EU Data Protection Directive 95/46EC through the Slovak Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending Certain Laws as of April 30, 2013, as amended (DPA).

This is the key piece of data protection legislation in Slovakia and applies generally to protect the rights of natural persons from unlawful interference with their private life as a result of personal data processing.

The Slovak Data Protection Office (Office) has issued two implementation decrees:

(i) Decree on the Extent of Safety Measures Documentation, published in the Slovak Collection of Laws under No. 164/2013; and

(ii) Decree on the Requirements of the Data Protection Officer, published in the Slovak Collection of Laws under No. 165/2013.

Any natural or legal person who systematically processes personal data, whether by automated means or by non-automated means (where the personal data constitutes or is intended to constitute part of a filing system), and who determines the purpose and means of the processing or provides the personal data for processing, is subject to the data protection rules contained in DPA.

A natural or legal person who is designated by law to process personal data for the purposes determined by law must also comply with the DPA.

The Slovak Republic has also implemented the EU Directive on Privacy and Electronic Communications 02/58EC, through the Slovak Act No. 351/2011 Coll. on Electronic Communications, as amended.

There is also sector specific regulation in certain fields that may apply in addition to the main data protection legislation. These sectors include telecommunications, health care and the financial and banking sectors.

The Office supervises compliance with data protection law in the Slovak Republic. It also maintains a register of data protection officers, investigates suspected breaches and can determine whether data protection laws have been breached. The Office may, at its sole discretion, impose a fine up to a maximum of € 200,000 for breach of obligations stipulated by DPA.

Protected data:

Personal data is defined as any information relating to a natural person, who can be identified, either directly or indirectly, in particular by reference to an identifier of general application (such as a birth number) or by reference to one or more characteristics or attributes specific to his/her physical, physiological, mental, economic, cultural or social identity. The concept of personal data under the DPA therefore includes a person's title, name and surname, address and other contact details, date of birth, birth number or other identifier of general application, as well as biometric data, information on personal features or background, or other attributes specific to a particular natural person.

The DPA exhaustively defines the concept of sensitive personal data. This includes information revealing a person's racial or ethnic origin, political attitudes, religion, membership of political parties or trade unions, and health. The processing of sensitive personal data is subject to stricter conditions and may even be prohibited.

Restrictions on transfer of data offshore:

Principle

Data can only be transferred to third countries that provide adequate levels of data protection.

EU/EEA, White List and Safe Harbour

Data can be transferred without authorisation to EU Member States and countries within the EEA. Personal data can be exported to White Listed countries, provided that the data controller provides the data subject with sufficient information regarding the processing that will be undertaken.

Personal data can also be exported to EU/US Safe Harbour certified organisations, provided that the transfer agreement meets the requirements laid down in the DPA. These include that the data transfer agreement must make provision in a number of specified areas, such as the purpose of the transfer of personal data and how the data will be stored.

Other countries

Data can be exported to other jurisdictions without the authorisation of the Office if one or more of a number of specified conditions is met. These include that the transfer is necessary for the performance of a contract for the data subject or the transfer is necessary to serve an important public interest.

Data can be transferred to third countries that do not ensure an adequate level of protection without the authorisation or consent of the Office provided that the data controller adopts measures to adequately protect the data, privacy and fundamental rights of the data subject. This can be achieved by using standard EU Model Clauses in the transfer agreement or Binding Corporate Rules that have been approved by the relevant data protection supervisory authority.

Slovenia

In Slovenia the collection, processing and use of personal data in the public and private sector is forbidden unless permitted by law. Slovenian data protection legislation is in line with the principles and requirements of the EU Data Protection Directive 95/46 EC and the EU Directive on Privacy and Electronic Communications 02/58 EC.

Applicable legislation:

Slovenia has implemented the EU Data Protection Directive 95/46 EC through the 2004 Personal Data Protection Act (as amended).

The right to privacy is also protected by the Slovenian Constitution. Article 35 of the Constitution guarantees a general right to privacy and Article 38 establishes a right to "informational privacy" under which every individual has a right to protection of his personal data. Article 38 also forbids data processing contrary to the stated purpose of data collection, and guarantees an individual the right to access the processed information and to judicial protection.

Slovenia has implemented the EU Directive on Privacy and Electronic Communications 02/58 EC through the 2012 Electronic Communications Act.

Data protection rules are also found in certain sector specific regulation. These include: the 2006 Banking Act (as amended), the 2007 Financial Instruments Market Act (as amended), the 2000 Insurance Act (as amended) and the 2013 Employment Relationship Act among others.

The Slovenian Information Commissioner has the power to issue civil monetary penalties of up to €1,000,000 for non-compliance with the 2004 Personal Data Protection Act. Other regulators responsible for ensuring compliance with the more sector specific regulation may issue civil monetary penalties of up to €400,000 for non-compliance.

Protected data:

Personal data is any data relating to an identified or identifiable natural person, irrespective of the form in which it is expressed. An identifiable natural 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, where the method of identification does not incur large costs, require disproportionate effort or a large amount of time.

Even more stringent protection applies to sensitive personal data, which includes data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health, sex life, appearance in or removal from criminal records, minor offences and biometric data.

Restrictions on transfer of data offshore:

EEA, White List and Safe Harbour

Data can be transferred within the EEA, to White Listed countries and to EU/US Safe Harbour certified recipients without the need for further authorisation.

Other third countries

Transfer is permitted to other third countries where: i) required by law or binding international treaty; ii) the data subject explicitly consents; iii) the transfer is necessary for the performance of a contract for the data subject; iv) the transfer is necessary for the protection of life or body; or v) the Slovenian Information Commissioner establishes that the data controller will ensures that the personal data and fundamental rights and freedoms of the individuals concerned will be adequately protected.

Where EU Model Clauses are applied in the transfer agreement with the recipient of the data, it is deemed that the personal data and rights of the individuals concerned are adequately protected. Although authorisation to export based on EU Model Clauses must still be sought from the Information Commissioner, the use of EU Model Clauses makes this authorisation much easier to obtain.

Spain

Spain has a developed general data privacy legislation broadly consistent with the principles in the EU Data Protection Directive 95/46 EC. These rules apply to the processing of any personal data by public or private entities.

Applicable legislation:

Organic Law 15/1999, of 13 December of Personal Data Protection.

Royal Decree 1720/2007, of 21 December, approving the Regulations developing Organic Law 15/1999, of 13 December of Personal Data Protection.

Final provision Fifty-six of Sustainable Economy Law 2/2011, of 4 March, has amended Organic Law 15/1999, of 13 December, on Personal Data Protection. The main modifications are as follows: (i) the amount of the fines imposed for minor breaches (from €900 to €40,000), serious breaches (from €40,001 to €300,000) and for very serious breaches (from €300,001 to €600,000); (ii) the criteria to classify penalties; and (iii) the power of the Spanish Data Protection Agency not to commence in certain exceptional cases disciplinary proceedings and, instead, require the party responsible for the offence to evidence that it has taken the corrective measures applicable in each case.

The Spanish Data Protection Authority is very active and publishes a large number of Legal Reports and resolutions which, together with the rulings from judges and courts, set the basis for the interpretation of the above legislation.

Protected data:

Information about living individuals which are identified or may be identifiable is protected.

The data protection legislation does not apply to information related to legal entities or sole traders, nor to files that only record data of individuals providing services in companies, comprising only their name and surname(s), functions or jobs performed, their postal or e-mail address and professional telephone and fax numbers.

A higher degree of protection applies to "sensitive information" relating to a person's ideology, trade union membership, religion, beliefs, racial origin, health or sex life.

Restrictions on transfer of data offshore:

The data controller shall obtain the prior authorisation of the Director of the Spanish Data Protection Authority to carry out transfers of personal data to a White Listed country.

There are several exemptions permitting an international transfer without obtaining authorisation from the Director of the Spanish Data Protection Authority, for example, obtaining of the free and unequivocal consent from every individual concerned. However these exemptions are interpreted restrictively by the Spanish Data Protection Authority. In any case, notification to the Spanish Data Protection Authority is required.

Sweden

Sweden has implemented the EU Data Protection Directive 95/46 EC into national law, which aims to protect the integrity of the individual. The Swedish data protection legislation is applicable to all processing of personal data with the exception of processing by a physical person of a private nature. The Swedish Data Inspection Board is the authority which monitors compliance with the Swedish data protection legislation.

Applicable legislation:

The Swedish Personal Data Act (1998:204) (the Act) and the Swedish Personal Data Ordinance (1998:1191) govern Swedish data protection law.

The processing of personal data may also be subject to further regulations under other legislation, e.g. in relation to marketing there are regulations under the Swedish Marketing Act (2008:486).

Furthermore, the Swedish Data Inspection Board issues ordinances regulating the processing of personal data.

Protected data:

The Act protects "personal data", which comprises all kinds of information that may, directly or indirectly, refer to a living person.

"Processing" of personal data under the Act means any action(s) taken regarding personal data, such as collection, recording, storage, adaptation or alteration, compilation, use or retrieval of personal data. The Act mainly applies to processing of personal data that (i) is wholly or in part automated, or (ii) forms or is intended to form a structured searchable collection.

The general principle under the Act is that consent needs to be collected from the data subject in order to process personal data lawfully. However, the Act contains several exemptions to this principle.

Restrictions on transfer of data offshore:

The Act prohibits the transfer of personal data (undergoing processing or for the purpose of processing) to countries outside the European Economic Area which do not guarantee an adequate level of protection, i.e. they have not been White Listed by the EU Commission.

However, such transfer is nevertheless permitted if the data subject has given consent to the transfer, or if the transfer is necessary for:

- the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the request of the data subject;
- the conclusion or performance of a contract between the data controller and a third party which is in the interest of the data subject;
- the establishment, exercise or defence of legal claims; or
- the protection of vital interests of the data subject.

In addition to this there are also a few very specific exceptions. If none of the exceptions apply, the use of the EU Model Clauses is the most pragmatic way to achieve compliant export of personal data.

Switzerland

The Swiss Federal Data Protection Act and its ordinances (Data Protection Act) applies to any personal data of natural persons and of legal entities (undertakings). It provides for rules on how personal data may be processed, such processing to include, in particular, irrespective of the methods and procedures applied, the collection, storing, alteration, use, disclosure, archiving or destruction of personal data, and the transfer to recipients outside of Switzerland.

The Data Protection Act applies to the private sector as well as to the Swiss Federal Authorities (including persons/institutions that provide for public services but are not authorities).

The general principles under the Data Protection Act state that personal data may only be processed lawfully. Its processing must be carried out in good faith and must be proportionate. Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law. The collection of personal data and in particular the purpose of its processing must be evident to the data subject. If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information.

Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.

Applicable legislation:

The collection and use of personal data is mainly governed by the Data Protection Act and the related data protection ordinances. In addition, certain provisions in other laws regulate processing of personal data. These laws include the Telecommunication Act, the Code of Obligations (data of employees), the Unfair Competition Act (anti-spam), the Banking Act, the Stock Exchanges and Securities Trading Act, the Act on Collective Investment Schemes and the Act on the General Part of Social Insurance. Some of these laws provide for secrecy obligations.

Switzerland is not a Member State of the European Union or the European Economic Area so the EU Data Protection Directive 95/46 EC is not applicable.

Protected data:

The Data Protection Act defines the following categories of protected personal data:

- "personal data": all information relating to an identified or identifiable person;
- "sensitive personal data": data on (i) religious, ideological, political or trade union related views or activities; (ii) health, the intimate sphere or the racial origin; (iii) social security measures; and (iv) administrative or criminal proceedings and sanctions; and
- "personality profile": a collection of data that permits an assessment of essential characteristics of the personality of a natural person.

Anonymous data (i.e. data that does not relate to an identified or identifiable person) is not subject to the Data Protection Act.

Sensitive personal data and personality profiles are subject to a higher level of protection and stricter rules.

Data security:

Personal data must be protected against unauthorised use by appropriate technical and organisational measures.

Restrictions on transfer of data offshore:

Personal data may not be transferred outside of Switzerland if the personality of the data subject is seriously endangered and any transfer of personal data abroad requires that the jurisdiction of the recipient guarantees an adequate level of data protection. The Data Protection Act contains the below comprehensive list of acceptable conditions that may ensure an adequate level of data protection abroad if the destination country does not have an adequate level of data protection laws:

- Sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad. Such clauses (agreements) or other safeguards must be notified to the Swiss Data Protection Commissioner (Commissioner).
- The data subject has consented in the specific case. As a general rule, consent must be given for each individual case.
- The processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party.
- The disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts.

- The disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject.
- The data subject has made the data generally accessible and has not expressly prohibited its processing.
- The disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection. Such rules must be notified to the Commissioner.

Turkey

Turkey does not have a single body of laws that protects the privacy of personal data, but personal information is protected through clauses in the Turkish Constitution and various criminal and civil laws.

Legislative reforms to implement the standards of the EU Data Protection Directive 95/46 EC are frequently introduced but have made little progress in the Turkish Parliament to date. At the time of writing, a new comprehensive bill is before the Council of Ministers and may soon be submitted to the Turkish Parliament for consideration.

Applicable legislation:

The Constitution provides the primary basis for the right to the protection of personal data.

According to the Constitution, every person has the right to demand that their personal data be protected. This right includes the right to be informed of any personal data that is kept about them, to have access to such data, to request the deletion or correction of such data, and to be informed as to whether such data is actually being used for the reason it was collected.

Personal data can only be processed if permitted by law or with the explicit consent of the person concerned.

The Criminal Code criminalises, among other things, the unlawful recording, retention, interception and dissemination of personal data, as well as the failure to destroy personal data after retention is no longer permitted by law. The law explicitly includes, within the definition of personal data, information on a person's political, philosophical or religious opinions, ethnic origins, and the details of their sex life, medical history and trade union connections.

The Civil Code provides the ground rules for the protection of privacy by stating that any person is entitled to request protection of their personal rights. Aggrieved persons may demand injunctions against such unlawful interventions, as well as pecuniary damages. The Code of Obligations mirrors the same rule and provides that an injured party may demand damages as well as injunctive relief in the face of a violation of their personal rights.

The Labour Code requires every employer to prepare a data file on each of its employees and to keep that file at the workplace for inspection by government inspectors upon demand. The law further states that the employer is obligated to use the information that it holds regarding its employees in good faith and in accordance with the law, and must refrain from disclosing such information if the employee has a justifiable benefit in keeping such information confidential.

Sector-specific restrictions apply to the collection and processing of personal data in certain regulated industries. For example, in the telecommunication industry, regulations impose obligations on electronic communications service providers to keep confidential the contents of electronic communications, information on its traffic and users' location information. Processing of communications traffic data and location information is permitted only with a view to aiding the resolution of disputes or addressing customer complaints. Marketing related or other value added processing of traffic data requires anonymisation and user consent. Processing of location data for providing value added services is similarly only permissible when anonymised, and requires informed consent. Consent based authorisations are strictly limited by the extent of the customer consent obtained, and customers must be able to withdraw consent through simple procedures and without charge.

Sharing this data with government agencies is only permitted where the recipient agency is specifically authorised by law to request such data. The agency must explicitly specify the reason for requesting the data and only on condition that the data is used for the purpose for which it was requested. Similar restrictions exist in the banking and healthcare industries.

There is currently no data protection authority in Turkey.

Protected data:

Protected data comprises all kinds of personal data including, but not limited to, information on a person's political, philosophical or religious opinions, ethnic origin, and the details of their sex life, medical history and trade union connections.

Restrictions on transfer of data offshore:

No specific restrictions exist in respect of the transfer of personal data to other countries.

However, the broad nature of the laws protecting personal data means that in practice the explicit consent of the person concerned is generally sought as a safe approach.

Sector specific restrictions, however, may prohibit the offshore transfer of personal data. Such a restriction was introduced in the telecommunications industry regulation in mid-2013, with effect from 1 January 2014. There are no exceptions to this restriction. The only leniency afforded was that the restriction came into effect five months after the remainder of the regulation.

United Kingdom

The United Kingdom has a comprehensive legislative regime that implements the EU Data Protection Directive 95/46 EC.

Applicable legislation:

England and Wales has implemented the EU Data Protection Directive 95/46 EC and the EU Directive on Privacy and Electronic Communications 02/58 EC through the Data Protection Act 1998 (the Data Protection Act) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 respectively.

Scotland and Northern Ireland are separate legal systems to England and Wales but have almost identical legislation to that in place in England and Wales. The UK Information Commissioner is the regulator for all three jurisdictions.

The UK Information Commissioner has powers to issue civil monetary penalties of up to £500,000 for non-compliance with the Data Protection Act.

Protected data:

Personal data is any data from which a living individual (the Data Subject) may be identified, either alone from that data or in conjunction with other information already in the possession of, or which is likely to come into the possession of, the person who determines the purposes for which personal data will be processed (the Data Controller) provided that, under current case law, such data is biographical of the Data Subject or focuses on the Data Subject.

Personal data primarily covers digital information but extends to some structured paper based records only, under current case law, where the organisation in control of the information also allows the searcher to find different categories of information about the individual without further analysis.

Restrictions on transfer of data offshore:

EU Data Protection Directive 95/46 EC grounds allowing transfer outside of the EEA or EU White Listed countries have been implemented, where the Data Subject has consented or where the processing is necessary to perform a contract with the Data Subject or another person and which is in the interests of the Data Subject. Otherwise, EU Model Clauses are the most straightforward route to achieve compliant export.

Ukraine

Ukraine is not a member of the EU so has not implemented the EU Data Protection Directives However, Ukraine's national personal data protection legislation is similar to the EU regime.

Applicable legislation:

The main piece of data protection legislation in Ukraine is the Law of Ukraine "On Personal Data Protection" No. 2297-VI, dated 1 June 2010, as amended (the Law).

The Ukrainian Parliament Commissioner for Human Rights (the Commissioner) enforces data protection legislation in Ukraine.

The Commissioner can: inspect data controllers; order that infringements of data protection laws are prevented and eliminated; suspend or terminate data processing activities; and submit administrative reports to courts for a data controller's administrative liability. Violation of personal data protection rules can be sanctioned by an administrative fine between UAH 1,700 to UAH 17,000 (approx. €110 to €1,100) per violation, depending on the type of violation. Breach of data protection laws may also lead to a criminal fine between UAH 8,500 and UAH 17,000 (approx. €550 to €1,100), up to two years corrective labour, up to six months arrest or up to three years' imprisonment.

Protected data:

The Law protects personal data, except where it has been depersonalised.

Personal data is defined as information about an individual who has been or may be specifically identified. It is treated as information with restricted access. Primary sources of personal data are documents that refer to a person or that have been signed by a person as well as information that an individual provides about him/herself.

Processing of personal data is defined widely as any action performed on the data and includes: collection, registration, accumulation, storage, adaptation, modification, updating and dissemination (distribution, sale, transfer), depersonalisation and destruction of personal data, whether by automated or non-automated systems.

Personal data can only be processed with an individual's consent, subject to exceptions where this is disapplied. Such exceptions include personal data processing for the purpose of national security: the protection of human rights; or if necessary for the protection of the vital interests of the data subject. However, these exceptions only apply until the consent of the data subject can be obtained.

Restrictions on transfer of data offshore:

Principle

The cross-border transfer of personal data is only allowed to countries that provide a proper level of personal data protection, as determined by Ukrainian legislation or international agreements. It is prohibited to transfer personal data offshore for a purpose other than for which the data was collected.

EEA and Convention 108 countries

EEA countries and parties to Convention 108 are deemed to provide a proper level of personal data protection. The Cabinet of Ministers of Ukraine also maintains a list of countries that provide a proper level of personal data protection.

Other countries

Data can be exported to non-Ukraine residents if one or more of a number of specified conditions is met. These include that the data subject explicitly consents, the transfer is necessary for the performance of a contract for the data subject and the transfer is necessary to serve an important public interest. There is no obligation to inform or seek the approval of any state authorities or the Commissioner on such transfer, unless the transfer constitutes a high risk to the rights of the subject of personal data.

The Americas

Argentina

Argentina has in place federal personal data protection laws, which are consistent with the EU Data Protection Directive 95/46 EC. The Argentine data protection laws apply to both governmental and private bodies that control databases containing personal information.

Applicable legislation:

Data protection is governed by the following laws in Argentina:

- Law No. 25,326 (Personal Data Protection Act) (the Data Protection Act);
- Decree No. 1558/2001 (the Decree); and
- Resolution No. 2/2005 issued by the National Office of Personal Data Protection (the Resolution).

The main purpose of the Data Protection Act is to protect data stored in public or private databases, in order to guarantee personal privacy and limit access to the data. The Decree and the Resolution regulate the Data Protection Act.

Among other things, the laws deal with what data can be collected and how it can be collected, used and stored. The laws also provide that an entity which keeps databases must register with the Ministry of Justice.

Protected data:

The laws prohibit the existence of databases that, directly or indirectly, may reveal sensitive personal data (such as race, religion, political preference, sexual preference or affiliation to trade unions).

The laws protect the information of people as well as non-physical entities that are identified in or identifiable from the data.

Restrictions on transfer of data offshore:

Argentina is a White Listed country. The European Union has recognised Argentina as a country with an adequate level of protection of personal data through the EU Data Protection Directive 95/46 EC. This recognition means that certain restrictions on the transfer of personal data do not apply to the country, and that the free flow of personal data from the European Union is allowed.

However, this recognition is subject to permanent control and can be reassessed at any time.

The Data Protection Act prohibits the transfer of data to countries or international organisations that do not sufficiently protect the data. However, the Decree authorises such transfer where express consent has been granted by the data subject.

This prohibition does not apply to:

- international judicial collaborations;
- exchanges of medical information for the treatment of the person affected;
- bank transfers or exchanges;
- exchanges of data within the framework of an international treaty to which Argentina is a party; or
- transfers to be used in an international cooperation between intelligence agencies to combat crime, terrorism and drug trafficking.

Brazil

Brazilian Law does not have any specific regulatory framework for data protection. There is, however, general legislation applicable which provides for the protection of the right to privacy and an individual's personal data.

Applicable legislation:

Brazilian Constitution of 1988 (Article 5, X) guarantees the right to privacy and (Article 5, XII) to secrecy of the content of mail and telephone conversations. Due to the lack of specific legislation addressing data protection, the Brazilian Congress and other government authorities have enacted laws and regulations addressing issues related to specific rights to privacy within their specific competence.

The Civil Code of 2003 (Article 21) also provides for the right of individuals to privacy.

The Executive Order no. 6,523 of 2008 regulates customer assistance channels and (Article 11) establishes that the consumers' personal data needs to be preserved and kept confidential.

The Consumer Code of 1990 (Article 43) also establishes that consumers must have access to all records related to personal data.

The right to privacy and to data protection is also present in employment legislation. Federal Law 9,029/1995 prohibits employers from requesting that female employees take pregnancy tests or submit proof of sterilisation or other related procedures to avoid discrimination. Article 508 of the Brazilian Labour Code had provided that employees at banks could be dismissed if they are insolvent regarding their personal debts, but this Article was revoked in 2010. Labour Courts have interpreted this revocation to mean that employers are prohibited from investigating or asking for employees' credit history, as well as from excluding applicants from selection processes based on the result of such investigations.

There are specific laws regulating the protection of tax and financial data (National Tax Code, Law 5, 172 of 1966) and banking financial privacy (Law 105 of 2001).

The right to privacy contained in the Constitution may be interpreted to apply in respect of all information of a personal nature, including personal data and private communications.

Law no. 9,029 of 1995 is intended to avoid discrimination against women in the workplace.

Restrictions on transfer of data offshore:

None.

Canada

In Canada, dovetailing federal and provincial laws govern the collection, use and disclosure of personal information in the private sector. These laws are based on principles consistent with the principles of the EU Data Protection Directive 95/46 EC. The Canadian privacy laws discussed below apply to the private sector. Additional privacy laws govern public sector agencies and governments in Canada and, in some provinces, specific privacy requirements that apply to hospitals and the healthcare sector. New federal legislation will strictly control the sending of commercial electronic messages.

Applicable legislation:

Federal legislation:
Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 (Canada) (PIPEDA); and

An act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c.23 (Canada) (Canada's Anti-Spam Law).

Provincial legislation:
Provincial privacy legislation that has been declared to be "substantially similar" to PIPEDA:

- Personal Information Protection Act, S.A. 2003, c. P-6.5 (Alberta);
- Personal Information Protection Act, S.B.C. 2003, c. 63 (British Columbia); and
- Protection of personal information in the private sector R.S.Q. c. P-39.1 (Quebec).

Additional privacy legislation applicable to health information and the healthcare sector that has been declared "substantially similar" to PIPEDA:

- Personal Health Information Protection Act, 2004, S.O. 2004, chapter 3 (Ontario);
- Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05; and
- Personal Health Information Act, SNL 2008 Chapter P-7.01.

Privacy legislation applicable to the private sector in Manitoba (the Personal Information Protection And Identity Theft Prevention Act) received Royal Assent on 13 September 2013, however is not yet in force.

In late Q3 of 2013, the Supreme Court of Canada declared Alberta's Personal Information Protection Act unconstitutional because certain provisions of that legislation were too broadly framed, constituting an undue limitation on freedom of expression. The court ultimately declared the entire statute to be invalid at the request of the Attorney General for Alberta rather than go through a provision by provision analysis. The Court gave the province twelve months to amend its privacy legislation to include safeguards that would properly balance the right to privacy and the right to freedom of expression. Other provinces will likely also be reviewing their privacy legislation to ensure no similar issues arise.

Protected data:

Generally speaking, Canadian private sector privacy laws are applicable to personal information which broadly means information about an identifiable individual. Typically, "business card" information is not considered to be personal information, although there remains an open question under PIPEDA and the Quebec legislation.

Security

The precautions that should be taken to protect personal information will be commensurate with the level of sensitivity of the information. Highly sensitive personal information (such as financial or medical information) is subject to the highest level of protection and security.

Restrictions on transfer of data offshore:

Applicable federal and provincial privacy legislation regulates, but does not prohibit, the transfer of personal information out of Canada. No additional consent need be sought for the cross-border transfer of personal information collected as long as the following conditions are met:

- the information is being used for the purpose it was originally collected and to which the subject already consented;
- the entity transferring the information ensures that a comparable level of protection of the personal information is provided by the receiving entity; and
- the persons concerned are notified that their information will be transferred outside the jurisdiction.

The Privacy Commissioner of Canada has considered the cross-border implications of outsourcing. She concluded that the cross-border transfer of personal information does not require additional consent from the individual concerned provided that the organisation is transparent and provides notice of the fact that: i) such transfers occur; and ii) once in the foreign jurisdiction, the information is subject to the power of the authorities in that jurisdiction.

The main provisions of Canada's Anti-Spam Law will come into force on July 1 2014.

This legislation is expected to have a significant impact on the sending of commercial electronic messages. Generally speaking, either express consent or consent that meets the statutory requirements of implied consent will be required in order to send commercial electronic messages.

Data is increasingly being processed and stored in the "cloud". Where such data includes personal information, it is essential for organisations to review and assess the adequacy of the security and privacy guarantees offered by the cloud provider. Such review may lead to the conclusion that the cloud is not suitable for the organisation's data storage and processing purposes.

Chile

In Chile, the basic principle of protection of personal data arises from Article 19, N° 4, of the Constitution which guarantees to all individuals the inviolability of any form of private communication. Private communications and documents may only be intercepted, opened or inspected in certain situations as determined by law.

Applicable legislation:

Protection of the Private Life Act:
Specifically, privacy and data protection are governed by the Protection of the Private Life Act, Law N°19.628, 1999 (the Law), which is applicable and mandatory to every public or private entity dealing with the gathering, recording, storage and management of personal data, including employers.

Law No. 20.575:
This law, enacted on February 17, 2012, amends Law No. 19.628 by regulating the treatment of such "personal data" specified in Chapter III of the Law, which relates to economic, financial, banking and commercial obligations and the companies which deal with these types of personal data, such as, Equifax and other similar companies.

Protected data:

The Law protects "personal data" which includes 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 by one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

According to the Personal Data Protection Act, any person can engage in the treatment and management of personal data, as long as it complies with the following rules:

- the treatment of personal data must be authorised in writing by the owner of the relevant information and authorisation may be revoked (with no retroactive effect) at any time;
- before any requirement to retrieve personal data by electronic means, the identity of the persons requiring such information, the purpose of the request and the type of information transmitted must be left on record;

- all personal data: that can no longer legally be stored must be eliminated; that is found to be mistaken, inaccurate, equivocal or incomplete must be amended; and that cannot be proven to be accurate or is in doubt must be blocked;
- all persons working, or who have worked, in the treatment and management of personal data must keep full confidentiality of the same;
- all personal data must be used exclusively for the purpose for which it was collected; and
- "sensitive data" cannot be subject to treatment, unless expressly authorised by the law, the owner or for the purpose of obtaining health benefits. "Sensitive data" means, with respect to a person, their physical or moral characteristics and facts or circumstances of their private life, such as personal habits, racial background, political opinions, religious beliefs, physical and mental health and sex life.

No authorisation from the owner of personal data is required in the following situations:

information generated by or collected from sources accessible to the public, of an economic, financial, banking or commercial nature;

information contained in lists regarding a category of persons limited to indicating the affiliation of a person to such category, its profession or activity, its education, address or date of birth;

information which is required for direct response commercial communications or direct sales of goods and services; and

treatment made by a private company for its own use or the use of its associates or affiliates, to determine tariffs, with statistical or other purposes for its own general benefit, of data related to its associates or affiliates.

In general, the owner of personal data is entitled to demand from any person engaged in the treatment and management of personal data to reveal any information pertaining to the former kept in the relevant data bank, and to amend, block or cancel such information, when applicable, at no cost. These rights cannot be curtailed by any covenant or agreement.

Elimination of data regarding obligations under 2,500,000 Chilean pesos, net value: Law No. 20.575 provides that the companies that treat personal data must eliminate from their records all obligations of individuals which as of December 2011 do not exceed 2,500,000 Chilean pesos, net value.

Restrictions on transfer of data offshore:

The Law does not contain restrictions in relation to transfers outside Chile, but fulfilment of the requirements described above should be observed.

Possible amendments to the Chilean Personal Data Protection Act:

Currently, there is a bill in the Chilean Congress (since late 2012) which aims to amend the Law. The bill's main purpose is to update Chilean regulations for the protection of personal data, and specifically, to reinforce the protection of private data with respect to third parties, and the fulfilment of the recommendation made by OCDE.

The main changes suggested by the bill cover the following matters:

- the scope of the law is re-defined, and new key definitions are included;
- inclusion of the "previous consent" concept and definition (Art.4);
- inclusion of the data protection principles recognised by OCDE;
- reinforcement of the "information right" that the data owner has, and the obligations of the person responsible and in charge of the data registry;
- inclusion of the duty to inform in commercial and advertisement communications: (i) where the personal data necessary to send such communication was collected; and (ii) the right of the owner of such personal data to avoid receiving such communications;
- regulation of the cross-border data flow;
- information duties of the registries and databases;
- inclusion of special protection of the personal data of children and teenagers;
- inclusion of a more efficient claim procedure;
- treatment of personal data by public institutions;
- creation of a violations and sanction index;
- creation of instruments that allow the fulfilment of the Law by creating prevention models and other methods to reduce fines; and
- creation of a market for certification entities.

The bill can be found at: http://www.camara.cl/pley/pley_detalle.aspx?prmID=8541.

Colombia

Colombia does not have a comprehensive law on data privacy equivalent to the EU Data Protection Directive 95/46 EC. However, the protection of privacy and personal data as well as the regulation of databases in Colombia is governed by Law 1581 of 2012 (as regulated by decree 1377 of 2013), Law 1266 of 2008 (as regulated by decrees 2952 of 2010 and 1727 of 2009), the Constitution and specific court rulings that have been issued to regulate the use of personal data.

Applicable legislation:

The Constitution of the Republic of Colombia (1991) provides privacy and data protection as fundamental rights, which means that individuals have the right to know, update and rectify information about them.

The main laws for data protection in Colombia are Law 1581 of 2012 and Law 1266 of 2008 which set forth the regulation of personal data that applies to individuals or companies in Colombia and generally to any data controller that uses personal data in Colombia.

Protected data:

Under Colombian Law and pursuant to Laws 1581 of 2012 and 1266 of 2008, personal data is any information that can be associated or linked to one or more determined or identifiable individuals or legal persons (Data Subjects).

Personal data includes:

- "public personal data": data is considered to be generally and freely accessible on request and contained in public documents or acts such as laws or judgments;
- "semi-public personal data": data with particular information connected to an identifiable person but without an intimate, reserved or public nature. Knowledge or disclosure of data is of relevance not only to the Data Subject, but to a specific sector or group of people or to society in general. This kind of data usually includes names, identification numbers and commercial activities;
- "private personal data": this information can only be released to the Data Subject, to parties with legitimate authorisation from the Data Subject and to parties with a judicial order mandating access;

- "reserved personal data": this refers to reserved or private information that is exclusively preserved for the private knowledge and management of the individual; and
- "sensitive data": information that concerns the intimacy of the Data Subject or information which, if abused, may generate discrimination related to racial or ethnic origins, political orientation, religious or philosophical convictions, membership to trade unions etc.

Restrictions on transfer of data offshore:

Pursuant to Law 1581 of 2012, personal data may not be transferred outside of Colombia to countries which do not comply with the adequate standards of data protections as determined by the Industry and Commerce Superintendent. This restriction does not apply:

- when there is an express authorisation by the Data Subject;
- when the information relates to medical data as required by issues of health and public hygiene;
- banking operations; and
- operations carried out in the context of international conventions which Colombia has ratified.

Mexico

Mexico has recently enacted a Data Protection Law (and corresponding Regulations) broadly consistent with international data protection principles. These rules apply to the processing (collection, use, disclosure or storage) of personal data by private entities except for: (i) government agencies; (ii) credit reporting agencies; and (iii) persons that collect and store personal data for their personal use. The processing of personal data by federal or local governmental agencies is governed by separate legislation.

Applicable legislation:

Federal Law on Protection of Personal Information in Possession of Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) (Data Protection Law) and its Regulation.

The Data Protection Law was published in the Federal Official Gazette on 5 July 2010 and came into effect on 6 July 2010, although some provisions related to privacy notices and enforcement of privacy rights did not become effective until 2011 or early 2012. The Data Privacy Law and its Regulations (published on 21 December 2011 and effective from 22 December 2011) are now fully in force.

On 17 January 2013, the Ministry of Economy (Secretaría de Economía) published some mandatory guidelines (Lineamientos del Aviso de Privacidad) for drafting privacy notices. These guidelines, which became effective on 17 April 2013, impose content requirements for privacy notices.

The Mexican data protection authority is the Federal Institute for Access to Public Information and Data Protection (Instituto Federal de Acceso a la Información y Protección de Datos) that has the authority to investigate compliance with and sanction infringements of the Data Protection Law by both governmental agencies and private parties.

Protected data:

Protected data includes any information pertaining to an individual (Data Subject) that it is identified or able to be identified. The Data Protection Law makes a distinction between "sensitive personal data", which refers to personal data regarding or affecting the most intimate aspects of an individual, and information that may have discriminatory effects or create serious risks for a person if put to unlawful use. "Sensitive personal data" includes: (i) racial or ethnic origin; (ii) current and future health; (iii) genetic information; (iv) political opinions; and (viii) sex orientation. The Data Protection Law also singles out "financial personal data" but it does not provide a definition of what constitutes "financial personal data".

Consent

As a general rule, personal data may only be processed with the Data Subject's prior consent. Data Subjects may grant consent expressly or in a tacit form for the processing of personal data.

Consent will be implied whenever the Data Subject does not reject the privacy notice made available by the data controller (individual or private entity that exercises decision-making power over the processing of personal data). Processing of financial or patrimonial data requires express consent (either oral or written) and processing of sensitive personal data will require express written consent.

Transfer of Data

As a general rule, Personal Data may be transferred to third parties as long as:

- such transfer was disclosed in the privacy notice and consented to by the Data Subject;
- the transferee received a copy of the privacy notice; and
- the transferee uses the personal data for the purposes disclosed in the privacy notice (the privacy notice must contain a specific clause indicating that the Data Subject authorises transfer to third parties).

It is important to bear in mind that the third party receiving the data may only use the personal data for the purposes disclosed in the privacy notice and shall be liable for the same obligations as those imposed on the data controllers.

Privacy Notice

As a general principle, personal data may only be used for the specific purposes disclosed in the privacy notice.

Whenever treating personal data, the data controller must provide the Data Subject with a privacy notice (privacy statement), which must include the following information:

- identification and address of the person treating the data;
- the purposes sought in the processing of Personal Data (including use and disclosure);
- determination if the personal data is sensitive or not;
- options and means to limit the use or disclosure of personal data;
- the procedure to exercise rights of access, rectification, cancellation or opposition;
- any transfer of data to be effected; and
- the notification procedure in the event of any significant change to the privacy notice. These requirements are further specified and expanded in the guidelines published by the Ministry of Economy on 17 January 2013.

Rights of Individuals

Data Subjects have and may exercise their rights in connection with their information, such as the rights of access, rectification, cancellation or opposition of their personal data. Every processing of personal data should be made with a reasonable expectation of privacy.

Restrictions on transfer of data offshore:

None, other than disclosing in the privacy notice that the data may/will be transferred offshore.

Sanctions

Offences under the Data Protection Law and related statutes can include fines (up to $1.6 million approx.). The Federal Institute of Access to Information and Data Protection (Instituto Federal de Acceso a la Información y Protección de Datos) has already initiated proceedings and imposed fines for considerable amounts against entities infringing the obligation to provide Data Subjects with a privacy notice.

Uruguay

Uruguay has comprehensive, detailed legislation regarding personal data processing. The legislation, which follows the EU Data Protection Directive 95/46 EC, applies to both public and private sectors, and in general prohibits the collection, processing and use of personal data, except with the prior explicit consent of the person concerned (Data Subject), or in certain exceptional situations specifically established by regulations.

In August 2012 the European Commission issued a decision stating that Uruguay provides adequate levels of personal data protection, declaring that international transfers of personal data towards Uruguay shall be considered as having the required safeguards.

Applicable legislation:

Given that personal data protection is considered to be a fundamental right of the individual, it is primarily protected by the Uruguayan Constitution.

In addition, personal data protection is governed by the Personal Data Protection and Habeas Data Action Law 18,331 of 11 August 2008, as amended by law 18,719 and law 18,996.

The Regulatory Decree 414/2009 contains further implementing provisions (the Regulation).

The Regulation establishes the rights and obligations that apply to personal data processing and specifies the conditions under which personal data may be transferred to other countries. It applies to:

- personal data treatment carried out by data controllers located within Uruguayan who perform their activities within the territory; and
- personal data treatment carried out by data controllers who are not located within Uruguay but who use for such treatment means situated in Uruguay, unless such means are used for transit purposes only.

Protected data:

The Regulation protects "personal data" which includes any information relating to any identified or identifiable individual and/or legal entity.

The precautions that should be taken in order to protect personal information ought to be proportional to the level of sensitivity of the information. Highly sensitive personal data is subject to the highest level of protection and security. Personal data is deemed to be sensitive when it relates to or is intended to relate to a person's racial or ethnic origin, political opinions, religious and/or moral convictions, trade union affiliations, sex preferences, health status and criminal records.

The Regulation contains a general requirement that personal data processing shall be allowed only with the prior consent of the Data Subject. However, it provides an exhaustive list of cases where consent of the Data Subject is not required.

It also establishes the main obligations that data controllers must comply with whenever collecting personal data. Accordingly, data controllers must inform the Data Subjects about:

- the purpose for which personal data will be collected, as well as the recipients or type of recipients of their personal data;
- the existence of a database where their data will be contained and the identity and address of the data controller;
- whether providing personal data is optional or compulsory, especially regarding sensitive data;
- the consequences of both providing their data and refusing to do so, as well as providing inaccurate data; and
- the possibility of exercising their rights of access, updating, rectification, inclusion and suppression or blocking of their personal data.

Restrictions on transfer of data offshore:

The Regulation prohibits the transfer of personal data to countries or international organisation that do not guarantee an adequate level of data protection and ensure its effective implementations according to international or regional standards.

The Uruguayan Data Protection Authority has recently passed a ruling stating that the countries that would be considered as complying with the required levels of data protection are those belonging to the European Union, as well as those considered by the latter as providing adequate levels of protection. Accordingly, international transfers of personal data to such countries will be lawful.

Otherwise, transfers of personal data offshore are only permitted if the conditions set out in the Regulation are complied with. International transfers of personal data to the US are permitted, even though that country is not considered to provide the required levels of data protection, provided that the recipient company is covered by the EU/US Safe Harbour.

United States

In the United States, no comprehensive federal data protection law exists. However, federal and state statutes and regulations address personal information privacy and data security, both generally and on an industry-sectoral basis to which every affected business must adhere, in addition to self-regulatory frameworks.

Applicable legislation:

The United States Constitution has been interpreted to provide protections against government infringement of certain privacy rights of individuals.

The United States has at least 19 federal laws that relate to privacy. Six of the broadest federal laws (and related regulations) are:

Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 et. seq. and implementing regulation at 16 C.F.R. Part 312.

COPPA places restrictions on companies that operate websites or provide online services directed at children under the age of 13, and those that have actual knowledge that they are collecting personal information online from children under 13. Those site operators must obtain parental consent before obtaining and using a child's personal information. COPPA includes a strict liability standard for site operators with respect to certain third party actions.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), 15 U.S.C. § § 7701-7713, applicable to commercial electronic messages.

CAN-SPAM covers e-mail and some text messages whose primary purpose is advertising or promotion of a commercial product or service, including contents of a website. The law typically does not cover "transactional" or "relationship" messages such as e-mails that facilitate an agreed-upon transaction (e.g. receipt for goods ordered) or update a customer on an existing business relationship (e.g. order has been delayed). Even these messages are prohibited from using false or misleading routing information.

CAN-SPAM has five basic requirements:

- the message must have accurate header information;
- the message must not have false or misleading subject lines;
- the message must contain a valid physical postal address;
- the message must provide the user with functional opt-out ability; and
- the sender cannot contact an individual after receiving an "opt-out."

Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681 et. seq.

FCRA provides consumers with certain rights relating to uses and disclosures of "consumer reports." "Consumer reports" are broadly defined to include "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (a) credit or insurance to be used primarily for personal, family, or household purposes; (b) employment purposes; or (c) any other purpose authorised" under the law 15 USC § 1681a.

Federal Trade Commission Act (FTCA), 15 U.S.C. § 41 et. seq.

This statute provides the Federal Trade Commission (FTC) with enforcement authority for the FTCA's prohibition of "unfair or deceptive acts or practices in or affecting commerce." The FTC has brought dozens of regulatory actions relating to explicit or implicit privacy claims about consumer and employee privacy.

Gramm-Leach Bliley Act (GLBA), Subchapter I (Disclosure of Non-public Personal Information) 15 U.S.C. §§ 6801-6809.

GLBA requires financial institutions (companies that offer consumers financial products or services like loans, financial or investment advice, or insurance) to explain their information sharing practices to their customers and to safeguard sensitive data. GLBA permits financial institutions to share non-public personal information with third parties provided that the financial institutions: (i) first offer consumers the ability to opt-out of such sharing; and (ii) have an agreement with the third parties requiring them to keep the personal information confidential.

Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-19 §§ 262 & 264 (see especially 42 U.S.C. §§ 1320d-1320d-9); and implementing regulations at 45 C.F.R. Parts 160 &164 HIPAA.

The HIPAA specified three topics of patient data that the new legislation or regulations were required to address:

- the rights that an individual who is a subject of individually identifiable health information should have;
- the procedures that should be established for the exercise of such rights; and
- the uses and disclosures of such information that should be authorised or required.

Among HIPAA's comprehensive and detailed regulations, the Privacy Rule sets national standards for the protection of certain health information, as applied to the three types of "covered entities": health plans, health care clearing houses and health care providers.

HIPAA's Security Rule focuses on protecting information from identified threats. The Security Rule divides these protective measures into three general types: "administrative, physical, and technical safeguards in an information system." In general, the Security Rule requires covered entities to:

- ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits;
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
- ensure compliance by its workforce.

State Security Breach Notification Laws:
Among the 50 states and the District of Columbia, only Alabama, Kentucky, New Mexico, and South Dakota do not have a law that requires notification of breach of personal information. Variance between and among the state laws is widespread.

Any suspected breach situation will need to be analysed based upon its unique facts and the laws applicable.

Alaska – Alaska Stat. § 45.48.010 et seq.

Arizona – Ariz. Rev. Stat. § 44-7501

Arkansas – Ark. Code § 4-110-101 et seq.

California – Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82

Colorado – Colo. Rev. Stat. § 6-1-716

Connecticut – Conn. Gen Stat. 36a-701b

Delaware – Del. Code tit. 6, § 12B-101 et seq.

District of Columbia – D.C. Code § 28- 3851 et seq.

Florida – Fla. Stat. § 817.5681

Georgia – Ga. Code §§ 10-1-910, -911

Hawaii – Haw. Rev. Stat. § 487N-2

Idaho – Idaho Stat. §§ 28-51-104 to 28-51-107

Illinois – 815 ILCS 530/1 et seq.

Indiana – Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.

Iowa – Iowa Code § 715C.1

Kansas – Kan. Stat. 50-7a01, 50-7a02

Louisiana – La. Rev. Stat. § 51:3071 et seq.; La. Admin. Code tit. 16, § 701

Maine – Me. Rev. Stat. tit. 10 §§ 1347 et seq.

Maryland – Md. Code, Com. Law § 14-3501 et seq.

Massachusetts – Mass. Gen. Laws § 93H-1 et seq.; 201 Mass. Code Regs. tit. 17

Michigan – Mich. Comp. Laws § 445.72

Minnesota – Minn. Stat. §§ 325E.61, 325E.64

Mississippi – 2010 H.B. 583

Missouri – Mo. Rev. Stat. § 407.1500

Montana – Mont. Code §§ 30-14-1704, 2-6-504

Nebraska – Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807

Nevada – Nev. Rev. Stat. §§ 603A.010 et seq., 242.183

New Hampshire – N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21

New Jersey – N.J. Stat. 56:8-163

New York – N.Y. Gen. Bus. Law § 899-aa

North Carolina – N.C. Gen. Stat § 75-65

North Dakota – N.D. Cent. Code § 51-30-01 et seq.

Ohio – Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192

Oklahoma – Okla. Stat. § 74-3113.1 and § 24-161 to -166

Oregon – Oregon Rev. Stat. § 646A.600 et seq.

Pennsylvania – 73 Pa. Stat. § 2303

Rhode Island – R.I. Gen. Laws § 11-49.2-1 et seq.

South Carolina – S.C. Code § 39-1-90

Tennessee – Tenn. Code § 47-18-2107, 2010 S.B. 2793

Texas – Tex. Bus. & Com. Code § 521.03, Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224)

Utah – Utah Code §§ 13-44-101, et seq.

Vermont – Vt. Stat. tit. 9 § 2430 et seq.

116 Norton Rose Fulbright – April 2014

Global data privacy directory

Virginia – Va. Code § 18.2-186.6, § 32.1-127.1:05

Washington – Wash. Rev. Code § 19.255.010, 42.56.590

West Virginia – W.V. Code §§ 46A-2A-101 et seq.

Wisconsin – Wis. Stat. § 134.98 et seq.

Wyoming – Wyo. Stat. § 40-12-501 to -502

In addition, some U.S. territories have similar laws: Guam (9 GCA § 48-10 et seq.); Puerto Rico (10 Laws of Puerto Rico § 4051 et. seq.); and U.S. Virgin Islands (V.I. Code § 2208).

Self-Regulatory Frameworks:
EU/US Safe Harbor: provides a method for US companies to transfer personal data located in the European Union to the United States in a manner that is consistent with the EU Data Protection Directive 95/46 EC. To join the EU/US Safe Harbor, a company must be regulated by either the Federal Trade Commission or the United States Department of Transportation and must self-certify to the Department of Commerce that it complies with EU standards. The FTC primarily enforces compliance with the EU/US Safe Harbor Framework. EU/US Safe Harbor program requirements are available at http://export.gov/safeharbor/eu/eg_main_018476.asp

Children's Privacy Seal Program: COPPA includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final rule. The listing of the companies and organisations that have been approved is available at http://business.ftc.gov/content/safe-harbor-program

Protected data:

Personal data will vary based upon which law(s) and regulation(s) apply to each situation.

Restrictions on transfer of data offshore:

None, although some of the laws and regulations require: (i) protection of personal data during transfer; and/or (ii) agreements with the parties to which personal data is being transferred; and/or (iii) knowledge of the location of the personal data. The US medicare requirements contain certain attestation restrictions relating to sending data offshore.

Venezuela

Venezuelan Law does not have any specific regulatory framework for data protection. There is, however, general legislation applicable which provides for the protection of right to privacy and individual's personal data.

Applicable legislation:

Article 60 of the Constitution of the Bolivarian Republic of Venezuela protects the right to a private life and privacy. Article 48 establishes Habeas Data Protection and Article 28 guarantees the secrecy and confidentiality of private communications in all of its forms.

Venezuela does not have a general privacy law but there are provisions dealing with privacy rights in various laws, including: the Telecommunications Privacy Protection Law; the Data Messages and Electronic Signatures Law; the Special Law on Computer Crimes; the Working Environment and Working Conditions Law and Regulations Concerning the Use of Electronic Banking Services.

In addition, the Venezuelan National Assembly is working on a set of draft laws that will regulate and protect Data Privacy (the Data Protection and Habeas Data Draft Law and the Information Technology Draft Law).

Protected data:

In general, Venezuelan law protects:

- the right of any individual or legal entity to know about the existence of any registry containing information or data about him/her/it;
- the right of the individual to access of information;
- the right to respond, which allows the individual or entity to control the existence and accuracy of the information concerning him/her/it;
- the right to know the use and purpose of the collected information;
- the right to update the information;
- the right to correct incomplete or false data;

- the right to destroy incorrect data or data that affects the individual's rights in an illegitimate way;
- the employee's right to the non-disclosure of personal health or medical information; and
- the right to protect or to not disclose sensitive information, without any legal process or the pertinent legal documentation or authorisations.

Restrictions on transfer of data offshore:

None.

Africa

Angola

Constitutional protection, as well as a wide-ranging Data Protection Law are in place.

Applicable legislation:

The Data Protection Law (DPL) has been published in the Angolan Official Gazette as Law 22/11, of 17 June 2011.

The DPL lays down a general regime to regulate the processing of personal data in Angola, which includes the collection, transfer and use of personal data for any purpose whatsoever.

The processing of personal data, as well as any cross-border transfers of personal data, are subject to strict notification and authorisation requirements with the Angolan data protection agency (yet to be created). These requirements are applicable regardless of whether the entities to which the data is being transferred are part of the same corporate group as the transferring entity or not.

Failure to comply with the terms or duties set out in the DPL may be sanctioned with both civil and criminal liability, as well as with administrative fines of between US$65,000 and US$450,000.

The Angolan Constitution 2010 (Article 69) (the Constitution) establishes a general right for any person to access computerised data that relates to him or her. This is enforceable by means of a cause of action known as "habeas data". A person bringing an action for habeas data can also demand that such data be corrected or updated.

This provision also includes an express prohibition on processing personal data for discriminatory purposes when this data relates to a person's political, philosophical or religious beliefs, trade union membership, political affiliations, ethnicity or private life.

The Constitution prohibits transmitting personal data from one government institution to another, except where provided for by law.

The Angolan Civil Code (the Civil Code) further creates an additional general duty to respect the private lives of others. This provision aims to limit and restrict any interference with a person's right to privacy.

Protected data:

"Personal data" is protected generally under the Constitution, the Civil Code and the DPL, as described above. "Personal data" is defined in the DPL as any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person. Natural persons are deemed to be identifiable whenever they can be directly or indirectly identified through such information.

Restrictions on transfer of data offshore:

The rules and principles applicable to a transfer of personal data from Angola to a foreign country depend on whether the Angolan data protection agency (yet to be created) deems the country to which the data is to be transferred to provide an "adequate level of protection". Data may be transferred across borders to third parties, other data controllers or to data processors acting on behalf of the data controller. The DPL does not distinguish between cross-border transfers of data to data controllers of data processors.

If the country in question does provide an adequate level of protection, then a transfer of data to that country will merely require the data controller to notify the Angolan data protection agency of the same. If, however, the transfer is to a country which does not provide an adequate level of protection then the data controller must obtain a prior authorisation from the Angolan data protection agency. Authorisation will only be granted in a limited number of situations, including:

- where the data subject has given his/her express written consent;
- where the transfer is necessary to perform a contract to which the data subject is a party or to undertake preliminary steps before executing a contract with the data subject;
- where the intended recipient of the data in the relevant country enters into a contract with the data controller and undertakes to provide an adequate level of protection for the data; and
- where the transfer is to another company in one particular corporate group which has implemented Binding Corporate Rules on the privacy and protection of personal data.

Ghana

A new Data Protection Act was passed in May 2012. This Act established a Data Protection Commission to protect the privacy and personal data of the individual by regulating the processing of personal information and setting out the process to obtain, hold, use or disclose personal information and for related matters.

Ghana also has common law and constitutional privacy provisions which prevent anyone from interfering with the private communication of a person except in accordance with the law and as may be necessary in a free and democratic society for the public safety or economic wellbeing of the country, for the protection of health or morals, or for the prevention of disorder or crime or for the protection of rights or freedom of others.

Applicable legislation:

The following legislation implements the data protection in Ghana:

The Constitution of the Republic of Ghana, 1992 (the Constitution).

The Data Protection Act, 2012, Act 843.

The individual licence agreements issued by the National Communications Authority (NCA) to telecommunications service providers contain some limited provisions regarding the protection of data received by service providers in the course of their activities.

The Electronic Communications Act, 1998 also empowers the NCA to impose conditions and restriction on data transfer in the individual licences of telecommunication service providers.

Protected data:

The Constitution provides protection against interference with any person's private communication. Personal data is protected by the Data Protection Act, 2012.

Restrictions on transfer of data offshore:

None.

Kenya

In Kenya, specific data privacy provisions in relation to the information and communication sectors, including e-commerce, are contained in the Kenya Information and Communication Act (the Act) as read with the Kenya Information and Communication (Consumer Protection) Regulations (the Regulations). In addition, the Kenyan Constitution (the Constitution) broadly provides for privacy as a fundamental right. There is in general no protection of privacy at common law.

Applicable legislation:

Under the Act, it is an offence for licensed telecommunication operators (otherwise than in the course of business) to intercept or disclose intercepted messages sent through telecommunication systems or to disclose the contents of any statement or account specifying the telecommunication services provided.

The Regulations grant customers the right to personal privacy and protection against unauthorised use of personal information. Licensees are prohibited from monitoring, disclosing or allowing any person to monitor or disclose, the content of any information of any subscriber by listening, taping, storing or other kinds of interception or surveillance of communications and related data. Further, prior customer consent is required in order to sell or offer for free to third parties any information collected which concerns the customer.

The Constitution grants every person the right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communication infringed.

Protected data:

The Act provides for several offences in order to protect computer data including:

- unauthorised access to computer data;
- access to computer program or data with the intent to commit an offence;
- interception of any function/data within a computer system;
- unauthorised modification of computer data;
- unauthorised disclosure of passwords and access codes;
- unlawful possession of devices and data; and
- electronic fraud.

Restrictions on transfer of data offshore:

Subject to the provisions highlighted above, there are no specific restrictions on the transfer of data offshore.

Malawi

Malawi presently has constitutional privacy protection. It is also possible to commence an action in tort based on the equitable doctrine of breach of confidence. There is no other legislation specifically dealing with data protection or privacy. However, an "E-Bill" has recently been drafted that will provide for, amongst other areas, data protection. It is expected that it will be enacted into law during the course of 2014.

Applicable legislation:

The Constitution of the Republic of Malawi (the Constitution) gives every person a broad right to privacy.

The Credit Reference Bureau Act (the CRBA) was passed into law establishing the Credit Reference Bureaus (the Bureaus). The Bureaus are involved in compiling, processing and disseminating credit information among users (financial institutions are separately regulated under the regime imposed by the Financial Services Act). The Bureaus are, by law, obliged to establish controls and procedures in order to ensure the quality of its database and to preserve the confidentiality of its information. The Bureaus are, therefore, required by law to provide accurate, legitimate, reliable, truthful and current information of the account holder.

In terms of the control of the communication of data by the press, the Censorship and Control of Entertainment Act (the CCEA) prohibits, amongst other things, the printing, publishing, manufacturing of any publication, pictures, statue or record which is undesirable. "Undesirable" under the CCEA is defined as that which is obscene or indecent, offensive to religious convictions or feelings, contrary to the interests of public safety etc.

Protected data:

The right to privacy contained in the Constitution may be interpreted to apply in respect of all information of a personal nature.

Restrictions on transfer of data offshore:

Under the CRBA, a Bureau cannot transfer or provide credit information to any user outside Malawi except with the written consent of the Registrar.

Mozambique

Mozambique has constitutional privacy protections, together with civil and labour law restrictions on the interception and monitoring of communications. A new law on data privacy protection is currently under consultation but it is currently not clear when it will be submitted to parliament.

Applicable legislation:

The Constitution of the Republic of Mozambique 2004 (the Constitution) grants everyone a right to privacy, prohibiting the use of electronic means for individual registration and manipulation of any data allowing for identification of a person's political, philosophical or ideological convictions, religious faith, political party or trade union affiliation and private life. Access to archives, files and computer records or databases containing personal data related to third parties, and also the transfer of personal data from one computer file to another belonging to different services or institutions is forbidden except under a judicial order (Article 68 in conjunction with Article 71).

The Civil Code (Administrative Ordinance no. 22869 of 4 September 1967) (the Civil Code) establishes the general principle that everyone shall keep private any information concerning another's private life (Article 80).

The Labour Law (Law no. 23/2007 of 1 August 2007) (the Labour Law) ensures the protection of employees' personal data, prohibiting the transfer to third parties without the employee's consent (unless for legal reasons) of any private data obtained by an employer subject to a duty of confidentiality, as well as any other information the dissemination of which would breach the employee's privacy. The Labour Law further provides that the use of computer files and access to the personal data of a job applicant or employee shall be subject to specific legislation (Article 6 in conjunction with Article 9).

Protected data:

The right to privacy contained in the Constitution and in the Labour Law is deemed to include all information of a personal nature in electronic format. The Civil Code broadly provides for the protection of privacy, which may apply to electronic and computer data.

Restrictions on transfer of data offshore:

None.

Nigeria

The Constitution of the Federal Republic of Nigeria, 1999 (the Constitution) currently provides for the protection of the privacy of Nigerian citizens.

The Cyber security and Information Protection Agency Bill, 2008 (the Draft Bill) provides for the establishment of a Cyber security and Information Protection Agency which will broadly seek to investigate, detect and prevent cyber-crime, and will regulate the activities of service providers across the IT industry in Nigeria. The Draft Bill prohibits the interception of communications, except where required by law enforcement agencies. The Draft Bill is yet to be passed by the National Assembly into law.

Applicable legislation:

The Constitution gives every citizen the right to privacy.

The Nigerian Communications Commission (NCC) set up under the Nigerian Communications Act, 2003 regulates the telecommunications industry in Nigeria. The Consumer Code of Practice Regulations 2007 issued by the NCC provides that all licensees must take reasonable steps to protect customer information against "improper or accidental disclosure" and ensure that such information is securely stored. It also states that customer information shall "not [be] transferred to any party except as otherwise permitted or required by other applicable laws or regulations".

Protected data:

Section 37 of the Constitution provides that the privacy of citizens and their homes, correspondence, telephone conversations and telegraphic communications is guaranteed and protected. However, neither the Constitution nor any other Nigerian law provides for the manner in which the privacy of Nigerian citizens is to be protected.

Restrictions on transfer of data offshore:

There is currently no legislation preventing the transfer of data offshore. Notwithstanding the exceptions contained within the NCC and the Constitution (as noted above), Nigeria currently has no detailed data protection legislation.

South Africa

South Africa presently has common law and constitutional privacy protections together with restrictions on the interception and monitoring of communications. The Protection of Personal Act, 2013 (POPI), was signed into law in November 2013 but a commencement date has not yet been proclaimed. This law is heavily based on foreign legislation, in particular the United Kingdom's Data Protection Act 1998.

Applicable legislation:

The Constitution of the Republic (the Constitution) gives every person a broad right to privacy.

The Regulation of Interception of Communications and Provision of Communication Related Act, 2002 (RICA) prohibits the interception and monitoring of communications without the consent of a party to the communication unless specified grounds to do so exist.

POPI establishes minimum requirements which must be complied with when processing personal information.

Protected data:

The right to privacy contained in the Constitution includes all information of a personal nature.

The privacy of communications is also protected by the Constitution and RICA. Personal information will be protected by POPI.

Restrictions on transfer of data offshore:

Once POPI comes into force, the cross-border transfer provisions will need to be complied with before data containing personal information may be transferred offshore.

Tanzania

Tanzania presently has constitutional privacy protections along with restrictions on the interception and monitoring of communications.

Applicable legislation:

The Constitution of the Republic 1977, as amended, (the Constitution) gives every person a broad right to privacy in that every person is entitled to the respect and protection of their private communications.

The Electronic and Postal Communications Act, 2010 (the EPCA) imposes a duty of confidentiality on all members and employees of certain licensed communications service providers. The EPCA further prohibits the disclosure of any customer information that is obtained by a licensed communication services provider in the course of providing its services.

The Electronic and Postal Communications (Consumer Protection) Regulations, 2011 (the Regulations) state that a licensed provider of communications services may collect and maintain information on individual consumers where it is reasonably necessary for its business, provided that the data must be:

- fairly and lawfully collected and processed;
- processed for identified purposes;
- accurate;
- processed in accordance with the consumer's other rights;
- protected against improper or accidental disclosure; and
- not transferred to any party except as permitted by any terms and conditions agreed with the consumer, as permitted by any permission or approval of the Tanzania Communications Regulatory Authority or as otherwise permitted or required by other applicable laws.

Protected data:

The right to privacy contained in the Constitution relates to an individual person's family and matrimonial life and his private communications.

The privacy of communications is also protected by the EPCA and customer data collected by licensed communication service providers is protected by the Regulations.

Restrictions on transfer of data offshore:

Other than the restrictions that apply to licensed communications service providers, there is no law that prohibits or restricts off-shore data transfers. A draft Data Protection Bill was in production throughout 2013, however at the time of writing no date had been given for its publication.

Uganda

In Uganda there is no legislation aimed specifically at data privacy. However, there are certain constitutional and legislative protections.

Applicable legislation:

The Constitution of the Republic of Uganda, 1995 (the Constitution) provides for the right to privacy.

The right to privacy is also set out in the Access to Information Act (the AIA) and the Uganda Communications Act, 2013 (the Communications Act). The Communications Act enjoins all operators to ensure that there is no unlawful divulgence, interception or disclosure of private information, with a few exceptions.

The Regulation of Interception of Communications Act, 2010 (the RICA) aims to regulate lawful interception by security organisations (the authorised persons) [should be defined?] of certain communications in the course of their transmission through telecommunication, postal or other related services. Such authorised persons have a right to give a notice of disclosure to any person requiring them to disclose any protected information, as well as acquire a retention order in respect of any postal article and examine the same.

This official access to private communications and data is to be done through a monitoring centre (yet to be established). All service providers shall be required to give all necessary assistance with regard to such interception and failure to do so could result in penalties such as cancellation of their licenses and/or a fine.

The Computer Misuse Act, 2011 seeks to provide security for electronic transactions and information systems and further prevents unlawful access, interception or interference with any program or data without authorisation. It is also unlawful for a person or organisation to disclose any electronic data which they have access to. It allows a data controller to acquire a preservation order to preserve any data stored by way of information and communication technologies and in turn, a disclosure order to disclose any such preserved data for purposes of criminal prosecution.

The Electronic Signatures Act, 2011 places an obligation on the subscriber named in a certificate issued by a "certificate service provider" to exercise reasonable care to retain the "private key" and to prevent its disclosure to any person not authorised to create the subscriber's digital signature. A "certificate service provider" is defined to mean "a person that issues certificates and may provide other services related to electronic signatures". A "private key" is defined as the personal property of the subscriber who rightfully holds it.

Protected data:

All data of a personal nature, electronic or otherwise.

Restrictions on transfer of data offshore:

Generally data can be transferred with the consent of the person or institution concerned, whether the consent is implicit or explicit. However, depending on the nature of the data, there may be further restrictions applicable. For instance, with regard to an employee's details, any restrictions contained within the Employment Act, 2006 will also apply. In the case of financial information any restrictions contained within the Financial Institutions and Banking Act will apply to the transfer of financial data.

Zambia

Zambia has statutory privacy and data protection provisions (the Privacy Laws) in respect of personal information of any person as well as in relation to the private communications of any person. The Privacy Laws prevent anyone from interfering with the private communication of a person, as well as preventing the disclosure and use of personal information of any person that would have been obtained by a person or a "data controller". A "data controller" refers to a person, either alone or in common with other persons, who controls and is responsible for keeping and using personal information on a computer and electronically requests, collects, collates, processes or stores personal information of any person. The prevention on the interference, disclosure and use of personal information, as stated above, will be subject to exceptions permitted by the law as well as instances where the consent of a person concerned has been obtained to disclose or use their personal information.

Applicable legislation:

The Electronic Communications and Transactions Act, Act Number 21 of 2009 (the Electronic Communications Act).

Protected data:

The Electronic Communications Act prevents the disclosure and use of personal information of any person without their express written consent. It also places an obligation on a person who requests the personal information of another person (the Data Subject) to disclose the Data Subject the purpose for which the Data Subject's personal information is requested.

The intention of the Electronic Communications Act is to ensure that all persons concerned are consulted in relation to the use of their personal information as well as to ensure that their personal information is protected.

Restrictions on transfer of data offshore:

The Electronic Communications Act allows a person to use any personal information to compile profiles for statistical purposes and may freely trade such profiles and statistical data, as long as such data cannot be linked to any specific individual person by a third party. The Electronic Communications Act does not therefore place any restrictions on the transfer offshore of any personal information. There is, however, the qualification that the transfer of the personal information through profiles or statistical data should be done in such a way that an individual person cannot be linked to the personal information that will have been transferred. The intention is to ensure the protection of the personal information of the Data Subject where their personal information may have been used for a profile or for statistical purposes.

Zimbabwe

The Constitution in force as at April 2014 provides no specific data privacy protection. The common law recognises in general terms a right to privacy, and affords a basis for a claim by a party aggrieved by a wrongful infringement of privacy.

Applicable legislation:

The Access to Information and Protection of Privacy Act (Chapter 10:27) provides, with certain exceptions, restrictions on the use and disclosure of personal information by a number of public bodies, including professional associations, medical aid societies and public companies.

The Census and Statistics Act (Chapter 10:29), inter alia, deals with the conducting of statistical surveys, and the use to which the results of such surveys can be put.

The Postal and Telecommunications Act (Chapter 12:05) makes it an offence for any employee of a telecommunication licensee or cellular telecommunication licensee to make use, for his own purposes, of information acquired relating to the contents of a communication.

The Interception of Communications Act (Chapter 11:20) allows certain authorised governmental authorities to apply for and obtain a warrant for the interception of communications sent by radio, telecommunication or by post, subject to certain restrictions.

Protected data:

Subject to the above, there is no specific legislation dealing with data protection.

Restrictions on transfer of data offshore:

None.

Middle East

Afghanistan

Afghanistan does not currently have any specific data protection laws in place and privacy protection under the general law is undeveloped.

Applicable legislation:

The Constitution of Afghanistan (the Constitution) does address personal privacy. Article 37 of the Constitution protects the right of citizens from having their private correspondence and communications from being interfered with in any way.

Article 37 of the Constitution provides for "Freedom and privacy of correspondence and communications of all persons are safe from invasion whether it is in the form of writing, telephone conversation, telegraph or any other means".

In addition to the above, Article 38 of the Constitution protects citizens residence from unlawful interference or invasion. "No one (including the government) can enter or search the private residence of a citizen without the permission of the dweller or dictum of a competent court (or other conditions described in law)".

The Ministry of Interior and the Ministry of Communication and Information Technology have announced that they intend to issue National Identification Cards (NID) but there is no clear timetable for this. It is unclear whether the creation of the NID will lead to any laws which will deal with the protection, handling or privacy of data held by the government.

Protected data:

See above for types of information protected.

Restrictions on transfer of data offshore:

No specific restriction.

Bahrain

There are few specific data protection laws in Bahrain, although the Kingdom has given more focus to this issue over the past few years. Both adults and children in Bahrain are facing more and more exposure to cyber-crime, cyber-bullying and unwanted contact online, according to the Bahrain Telecommunications Regulatory Authority (TRA), which released its first State of the Nation Review on information and communications technology safety in 2011.

Draft laws are under consultation and some established laws also offer indirect protection of privacy. In particular, laws and consultations relating to the use of private data as an advertising tool, and the implementation of sanctions where private data has been accessed, published, used and/or communicated without approval.

Applicable legislation:

The Guidance Paper on TRA Treatment of Confidential and Non-Confidential Information dated 10 September 2007 states that the TRA takes seriously the treatment of confidential information and has an obligation not to divulge any confidential information under Section 23 of the law promulgated by Legislative Decree No. 48 of 2002 (the Telecommunications Law). A breach of confidentiality may lead to the penalties as described in the Telecommunications Law and Bahraini law generally.

Regulation regarding Bulk Messaging (TRA Regulation No. 1 of 2011) was issued by the TRA on 24 February 2011. Bulk messaging has long been an issue in Bahrain, and the new law provides limited protection from the advertising activity of bulk messaging (by SMS and/or MMS) mule mobile phone numbers. Such messaging still occurs today but on a less frequent scale, and the introduction of a law targeting this issue certainly comes as a step forward in a country which had no such rules in place in the past.

The consolidated e-transactions law (Decree No.28 of 2002) enforced protection measures applicable to e-registers and e-signatures by implementing systems and control procedures relevant for the security, safety, e-register privacy, its ability to be verified and disposal. This law provides much needed protection and regulation, in particular concerning online safety such as protection of payment details and prevention of identity theft.

The Consumer Protection Guidelines (29 December 2011) clarified the position of the TRA in relation to privacy and confidentiality of data. In its sections 41 to 46 it states that licensed operators should take steps to protect consumers' privacy regarding personal information and calling patterns. Consumers should expect that their personal privacy will be protected from: unauthorised use of their personal records and information; and, illegal, unsolicited, unwanted or offensive communications.

The Kingdom of Bahrain has introduced a new piece of legislation in 2012 regarding Consumer Protection (Decree No. 35 of 2012). Art.2 (5) of the law provides the right to respect consumer privacy, maintain personal information and not exploit such information for other purposes.

The Bahrain Penal Code, Amiri Decree No. 15 of 1976, provides for criminal punishment for divulging a secret entrusted by a person concerned with such information without consent to disclose the same from such concerned person (Art. 371) and extends to use by the recipient for his personal benefit or the benefit of another.

In 2009, the TRA issued Resolution No. (8) promulgating a regulation requiring licensees to implement lawful access. The implementation is achieved by requiring licensees to provide all technical resources (including telecommunications equipment, systems, programs and communication links) which allow security organs to have access to the call content and access related information sent via the telecommunication network that it is licensed to operate for purposes of fulfilling the requirements of national security.

"Security organs" are defined as every entity that is concerned with any national or international security matter in accordance with the applicable laws and regulations of the Kingdom of Bahrain. This regulation makes private data available to security organs where required but also provides some regulation on the lawful access to such data.

Article 9 provides, among other things, that licensees shall undertake to retain access related information (such as IP address, mobile number, etc.) with full confidentiality.

In relation to telemarketing, licensed operators are expected to protect consumers from unwanted or illegal electronic solicitations, including live voice solicitations, artificial pre-recorded voice advertisements, electronic mail, electronic wireless messages (e.g. SMS, MMS) and facsimile messages. The Regulation regarding Bulk Messaging (TRA Regulation No. 1 of 2011) issued by TRA on 24 February 2011 further enforces such requirements.

The TRA has also introduced a guide for surfing the internet safely (http://www.safesurf.bh/index.html) which illustrates the commitment to achieve harmonised protection with the rest of the world.

All these improvements to data privacy rules in Bahrain will need to be coupled with further legal developments and the introduction of a system which actively regulates any breaches.

Despite there being a long way to go until Bahrain reaches the level of data protection existing in other developed countries, a step in the right direction has been taken and the government agencies seem committed to introduce further measures.

Protected data:

Confidential information is defined in the Guidance Paper on TRA Treatment of Confidential and Non-Confidential Information dated 10 September 2007. For the purposes of the

Telecommunications Law (Art. 23), the TRA will only consider information possessed by a person to be confidential where:

- the information is not or has not been publicly circulated or published by the person;
- the information is not readily accessible to persons in the telecommunications market or is not otherwise in the public domain; or
- the information has a commercial value or, relates to personal particulars or private affairs of a natural person.

In accordance with the Consumer Protection Guidelines of 29 December 2011 and subject to any obligations to disclose information in accordance with the laws of the Kingdom of Bahrain, licensed operators should maintain the confidentiality of, and refrain from using or disclosing, other than for the proper purposes of providing telecommunications services, any:

- confidential, personal and proprietary information obtained in the course of its business from any consumer, where such information originates from any such consumer;
- any information regarding usage of a telecommunications network or service; or
- information received or obtained in connection with the operation of a telecommunications network or the provision of a telecommunications service.

In relation to health records, a computerised Medical Records Tracking system has been developed. The system tracks the files from the medical records storage shelves through all the locations they are sent such as clinics, wards, admission office, doctors' offices, insurance companies and various additional locations until they are returned back to the shelves. The British Standards Institute (www.bsi.co.uk) has formalised information security management and issued the BS7799 Standards to provide a set of controls comprising best practices in information security. The BS7799 Standards which are accepted as ISO17799 provide a framework for developing an Information Security Policy. It is a strong reference point for identifying the range of controls needed for most situations where information systems are used in the business world. The Health Insurance Portability & Accountability Act is framing the law for data protection in the healthcare industry. Unfortunately, there are no such data protection laws in Bahrain, and it seems health care customers are therefore exposed to breaches.

According to the Bahrain Health Ministry, personal information is any information that is identifiable with a given person. This information may include, but is not limited, to a person's name, personal phone numbers and personal email address.

Restrictions on transfer of data offshore:

There are no specific laws restricting the transfer of data offshore.

Egypt

Egypt does not have any formal data protection laws. However, there is legislation in place that sets out specific confidentiality obligations relating to employee information, information on money laundering investigations, capital markets data and banking secrecy provisions.

Applicable legislation:

The Labour Law no. 12 of 2003 (the Labour Law) obliges an employee to provide certain information (such as name, address, military and social status) (Mandatory Information) be kept in the employee's file held by the employer and reviewed periodically by the relevant government authority. Article 77 of the Labour Law stipulates that only authorised individuals shall have access to review personal employee data.

Other than this stipulation, the Labour Law does not address further information that can be provided by the employee. We are of the opinion that the employer is entitled to ask the employee to provide further personal information as long as it is reasonably relevant to the job of the employee (such as health checks and so forth). The Labour Law is silent as to what happens if the employer divulges such extra personal information, but we are of the opinion that such extra information should be treated in the same way as Mandatory Information. In any case, the obvious solution if there is a certain need to divulge some such information is to obtain the written consent of the employee to such disclosure, preferably in the employment contract.

Article 97 of the Banking Law stipulates that all bank customer accounts, deposits, trusts, safes and their related dealings shall remain confidential. They may neither be reviewed nor may any details be disclosed, either directly or indirectly, except with the written permission of the owner of the account, deposit, trust or safe, his successors, anyone to whom all or some of such funds have been bequeathed, a legal representative or authorised attorney or pursuant to a judicial ruling or an arbitral award. Such prohibition remains in force even if the relationship between the customer and the bank is terminated for any reason.

The Anti-Money Laundering Law no. 80 of 2002 prohibits disclosure to clients or beneficiaries of a suspicious transaction that a notification or an investigation is taking place with regards to such transaction.

Article 309bis of the Penal Code sanctions whoever discloses or facilitates the disclosure of, or uses (even privately) a recording or document obtained by any of the following methods:

- recording or transmitting via private conversations or telephone by any method; or
- shooting, taking or transmitting a picture of anyone in a private place by any means.

In the event the above occurs without the consent of the concerned party, the violator shall be subject to imprisonment for up to three years.

Article 322 of the Capital Markets Law no. 95 of 1992 stipulates that persons that are familiar with internal information because of their positions or the nature of the tasks they perform, shall be prohibited from exploiting this information for their personal account or for account of third parties, or divulging this information to a third party, whether directly or indirectly. The Article 323 of the Capital Market Law states that divulging the secrets of a client's accounts and dealings, or carrying out any work which would prejudice the interest of the dealer or of third parties shall be prohibited. Dealing in a security shall be banned if the dealer is directly or indirectly cognisant of substantial information related to it and is aware that such information exists but is unannounced. Moreover, Article 324 of the Capital Market Law stipulates that a dealer in a security shall not be considered a user or a beneficiary of the internal information if it is established that his dealing was due to other reasons than his access, directly or indirectly, to the internal information.

In addition to the above, Article 57 of the new Egyptian Constitution (promulgated on the 18th of January 2014) (the Constitution) stipulates that the law shall protect the inviolability of citizens' private lives.

Correspondence, wireless, telephone calls and other means of communication shall have their own guaranteed sanctity and confidentiality which may not be confiscated or monitored except by a judicial warrant and even then only for a definite period and according to the provisions of the law. Article 99 of the Constitution stipulates that any assault on individual freedom or the inviolability of citizens' private lives and any other public rights and liberties guaranteed under the Constitution and the law shall be considered a crime, whose criminal and civil lawsuit shall not be liable to prescription and pursuant to which the state shall grant a fair compensation to such victim. The same article also states that such victim may directly start criminal action against the perpetrator(s). However, the constitutional provisions do not create on their own direct obligations on individuals, but impose an obligation on the state to issue laws that apply constitutional principles.

The most salient source of liability for clients is likely to be tortious liability, (i.e. a fault (divulgence of private data) where damage is suffered and a causal link exists between the damage and fault). Article 50 of the Egyptian Civil Code stipulates that a person whose inherent personal rights have been unlawfully infringed shall have the right to demand cessation of such infringement and compensation for any damage sustained thereby.

Protected data:

See above.

Restrictions on transfer of data offshore:

None.

Iran

Data protection is a new field under the Iranian legal regime and currently is not subject to extensive regulation. In Iran, there is no specific law on data privacy and the subject has been sporadically dealt with by other laws and regulations. Most of the legislation is fairly recent and further development of these laws is expected.

Applicable legislation:

Three particular laws containing provisions concerning the protection of data are: the Law on Electronic Commerce (LEC), approved in 2004; the Law on Computer Crimes (LCC), approved in 2009; and the Law on Publicising and Access to Data (LPAD), which entered into force in February 2010. Other laws and regulations also require protection of data within a specific context.

Private contracts for non-disclosure of information are generally acknowledged based on the freedom of contract principles recognised under the Iranian Civil Code.

According to Article 58 of the LEC, "storing, processing or distributing private data messages which may reveal tribal or ethnic origins, moral and religious beliefs, ethical characteristics and data messages regarding the physical, psychological or sexual condition of people, without their explicit consent is illegal."

A "data message" is defined as any representation of facts, information and concepts generated, sent, received, stored or processed by use of electronic, optical or other information technology means.

Violation of the above rules is punishable by a prison sentence of one to three years.

Article 16 of the LCC provides that anyone who, by use of computer or telecommunication means, publicises or makes accessible the film or picture or sound or personal or family secrets of another person without his or her consent and causing loss or damage to the relevant individual or violating that person's dignity will be sentenced to imprisonment for between 61 days and six months or fined Rls 1,000,000 to 10,000,000. Unauthorised access to and distribution of secret information (i.e. information which, by its disclosure, would harm national security or the public interest) is also an offence under the LCC.

Under the LPAD, data is defined as "any data incorporated in a document, or saved in the form of a software or recorded through any other medium". LPAD categorises the data into "private information" (including personal information such as first name and surname, home and work addresses, individual habits, bank accounts etc.) and "public information" (such as

rules and regulations, national and official statistics and figures etc.). According to LPAD, while private information can only be accessed by the person to whom the data belongs or from the authorised proxy, public information can be accessed freely (except in cases prohibited by relevant laws).

LPAD recognises the right of persons to claim damages (based on the Law on Civil Liability) in case any loss or damage is suffered as a result of the publication of untrue data or true data in breach of the provisions of the law. A breach of LPAD is regarded as a crime resulting in a financial penalty of a sum between Rls 300,000 and Rls 100,000,000. Where other laws impose higher penalties for the same offences, the higher penalty will apply.

In addition, the Islamic Punishment Act penalises the disclosure of information obtained by doctors, pharmacists, surgeons and other trusted people in the course of carrying out their work. The collection of classified information to distribute is also an offence in certain circumstances.

Protected data:

Private "data messages" that may reveal a person's tribal or ethnic origins, moral and religious beliefs or ethical characteristics, or contain information regarding the physical, psychological or sexual condition of individuals are protected by the LEC.

Personal or family secrets are protected by the LCC.

Provisions of the LEC and LCC apply only to data processed in an automated fashion, whereas the Islamic Punishment Act includes data processed in automated fashion, hard copies and any other means.

The LPAD protects data as described in the preceding section.

Restrictions on transfer of data offshore:

There is no explicit restriction.

Iraq

There is currently very limited provision in law relating to data protection in Iraq, though individual licences granted to operators in the information services and communications sector may include data processing provisions.

The Constitution of Iraq passed in October 2005 (the Constitution) addresses personal privacy. Article 17 (1) of the Iraq Constitution states that: "Each individual has the right to personal privacy, as long as it does not infringe on the rights of others or public decency."

There is little available guidance on this constitutional provision. The right to privacy was not defined by legislation prior to the enactment of the Constitution and has not yet been defined in legislation since its enactment.

Two proposed pieces of legislation (the Information and Communications Law and the Information Crimes Law) may contain provisions relating to the protection of personal data. However, these have been under consideration for some time and there is no indication as to when they will be enacted. In July 2013, both laws were put on hold by the Iraqi parliament and sent back to the government for redrafting.

Applicable legislation:

Iraq does not currently have any specific data protection laws in place and privacy protection under general law is fairly undeveloped. There is reference to a "right to personal privacy" in the Constitution but little available guidance on this constitutional right, which has not yet been defined in legislation.

The Iraqi parliament is reviewing certain data privacy related laws, but there is no clear timetable for enactment. It is unclear when and if these laws will come into force or whether it might be subject to extended debate and amendment.

The information services and communications sector is regulated by the Iraqi Communications and Media Commission (the CMC) as established under Coalition Provisional Authority Order No. 65. As a matter of practice, the CMC may include data processing provisions in licences granted to operate in that sector.

Protected data:

Not applicable.

Restrictions on transfer of data offshore:

Not applicable.

Israel

The protection of privacy and personal data in Israel and the regulation of databases in Israel are governed by the Basic Law: Human Dignity & Liberty (the Basic Law) and the Protection of Privacy Law, 1981 (the Privacy Law) and the applicable regulations enacted thereunder.

On January 31, 2011, the EU resolved that Israel is considered as providing an adequate level of protection for personal data transferred from the EU in relation to automated international data transfers or, in the event that they are not automated, where they are subject to further automated processing in Israel.

Applicable legislation:

The Basic Law sets out in general terms the fundamental rights of any person to privacy and to intimacy and further protects in general the privacy and secrecy of a person's communications. The Privacy Law sets out in detail provisions for the protection of personal information. These include a number of substantive issues concerning, inter alia, the processing, collecting, transferring and maintaining of such information in Israel.

In addition, applicable regulations have been enacted under the Privacy Law. Such regulations regulate, inter alia, the transfer of information from a database in Israel to outside of Israel (the Protection of Privacy Regulations (the Transfer of Information to a Database Outside the State Borders) 2001), data protection (the Protection of Privacy Regulations (Conditions for Keeping and Protecting Information and Procedures for Transfer of Information between Public Bodies) 1986) and viewing information (the Protection of Privacy Regulations (Conditions for Viewing Information and Procedures on Appeal against Refusal to Allow Viewing) 1981).

Protected data:

With respect to any information held in a database in Israel, the Privacy Law sets out legal requirements which must be complied with if applicable regarding, inter alia, registration, notification, data security, collection and processing of data, confidentiality, appointment of a security officer etc.

In this regard, "data" is defined in the Privacy Law as information about an individual's personality, personal status, intimate affairs, health condition, financial condition, professional qualifications, opinions and beliefs. The Privacy Law further refers to "sensitive data", which is defined as data on an individual's personality, intimate (i.e. private) affairs, state of health, financial condition, opinions and beliefs. There are different registration requirements with respect to sensitive data.

In addition, the Privacy Law also includes general provisions regarding privacy which are not restricted only to databases. Such provisions refer to additional types of protected data. These include, for example, a determination that using, or passing onto another, information about a "person's private affairs", other than for the purpose for which such information was provided, constitutes a breach of privacy.

In this regard, it should be noted that the Israeli courts have interpreted the terms "data", "sensitive data" and "person's private affairs" broadly.

Restrictions on transfer of data offshore:

The transfer outside of Israel of data from a database in Israel is regulated by the Protection of Privacy Regulations (The Transfer of Information to a Database Outside the State Borders), 2001 (the Regulations).

The Regulations prohibit the transfer of information from a database in Israel to a database located abroad, unless the receiving country in question ensures a level of protection of information which is not lower than the level of protection provided for under Israeli law.

In addition, the Regulations lay down several conditions which enable the transfer of information from a database in Israel to a database abroad, even when the law of the state in which the data is received provides a level of protection which falls below that which is provided for under Israeli law. Upon the fulfilment of any one of the following conditions the transfer of information, as aforementioned, shall be permitted:

- on the receipt of the consent to the transfer of the information from the person who is the subject of the information;
- if it is not possible to obtain the consent of the person who is the subject of the information, but its transfer is absolutely necessary in order to protect his/her health or the integrity of his/her physical body;
- where the information is being transferred to a corporation under the control (i.e. the ability to direct the activities of an entity) of the owner of the Israeli database and it has ensured the protection of privacy following the transfer;
- where the information is being transferred to someone who has undertaken in an agreement, with the owner of the Israeli database, to fulfil the conditions laid down in Israel for the maintenance and use of the information, mutatis mutandis;
- where the information has been made public by the lawful authority, or it has been made available for inspection by the public under lawful authority;
- where transferring the information is essential for the defence of public welfare and security;

- where transferring the information is required by a statute in Israel; or
- where the information is being transferred to a database in a country in which any one of the following conditions exist:

(i) it is a party to the European Convention for the Protection of Individuals in connection with automatic processing of sensitive information;

(ii) it receives information from member states in the European Union, under the same conditions of receipt; or

(iii) the Registrar of Databases has notified with respect to the country, in a notification which has been published in the Official Gazette, that there exists in such country a designated authority to protect privacy, after it has reached an arrangement for cooperation with such authority (at the date of publication, the Registrar of Databases had not issued any such notification).

In addition to the fulfilment of the above conditions, the Regulations state that the owner of the database must ensure (by way of a written obligation from the recipient of the information), that the recipient is taking steps to ensure the privacy of the person to whom the information relates, and that the recipient undertakes that the information shall not be transferred to any person other than himself/herself, whether or not such person be in the same country.

In general, any transfer of data from a registered database outside of Israel should be undertaken in accordance with the registered purpose of the database and the information that was provided in this regard during the registration process of the database, and subject to receipt of required consents, if applicable.

Jordan

Jordan has not legislated any data privacy laws but has certain privacy requirements for particular matters such as banking.

Applicable legislation:

Banking

All matters that deal with bank secrecy are governed and regulated by the Banking Law No.28 of 2000 (the Banking Law). Article 72 of the Banking Law imposes strict confidentiality obligations on any bank operating in Jordan (including registered branches of foreign banks) in connection with any information relating to its customers' transactions, accounts, funds, operations and dealings as far as such transactions and dealings do not violate any laws and regulations in force. Accordingly, a registered Jordanian bank is prohibited from providing, whether directly or indirectly, any information on any of its customers, unless certain exemptions listed in Article 72 and 74 of the Banking Law apply.

According to Article 75 of the Banking Law, in the event a bank (or another relevant party) breaches the confidentiality obligation, the party that violated such provision shall be punished by imprisonment for a period not less than six months and/or a fine between JOD 10,000 and JOD 50,000.

Employment

Article 814 of the Jordanian Civil Code No.43 of 1976 (the Civil Code) imposes on an employee an obligation to keep all the employer's commercial and industrial secrets confidential even after the termination of the employment contract (as per the terms of the employment contract or the customs governing the industry). Furthermore, Article 28 of the Jordanian Labour Law No.8 of 1996 (the Labour Law) states that an employer may dismiss an employee in the event the employee divulged the employer's trade secrets.

Professionals

Members of professional associations such as doctors, pharmacists and lawyers are obliged to keep their clients' information confidential by virtue of their respective association's laws (e.g. Agricultural Engineers Association Law No.19 of 1998).

Protected data:

Please see above.

Restrictions on transfer of data offshore:

No specific restriction.

Kuwait

The State of Kuwait has yet to enact a separate data protection/privacy statute analogous to the comprehensive legislative schemes found in certain other jurisdictions such as the United Kingdom. However, certain areas of Kuwait law are generally considered to encompass aspects of data protection.

Applicable legislation:

Article (39) of the Constitution of the State of Kuwait provides that:

"Freedom of communication by post, telegraph and telephone and the secrecy thereof shall be guaranteed; accordingly, censorship of communications and disclosure of their contents shall not be permitted except in the circumstances and manner specified by law".

Based on this, any information that is transmitted by post, telegraph and telephone would be considered confidential and may only be disclosed to the public in accordance with Kuwait law.

Article 43 of the Evidence Law No. 39 of 1980 stipulates that "lawyers, doctors, agents or others who acquire information in the course of carrying out their professions may not reveal the same, even after the end of their services or their representative capacity, unless such information was relayed to them with the intention of committing a felony or a misdemeanour". Accordingly, a reasonable argument may be made that businesses that come to know personal information about their consumers or clients fall within the "others" category and may not therefore reveal their consumers' or clients' personal information acquired in the course of business.

The Central Bank of Kuwait Circular dated December 2, 1986 (the Circular) declared that banks fall within the category of "others" under Article 43 (referred to above) and that bank officers and employees may not reveal information about their customers or any information received about customers of other banks in the course of their business. The Circular also provides that a bank would be responsible for the actions of its officers and employees who violate such duty of confidentiality.

Although Kuwait's Civil Code lacks provisions specifically relating to data protection, Article 227 thereof creates liability in damages on the part of any person who, by a "wrongdoing", causes harm to another person. Such "wrongdoing" would conceivably cover those circumstances involving misuse or misappropriation of another's personal data. This provision may be used as a basis for bringing an action in damages relating to invasion of privacy or misuse of information.

Generally, in collecting, using, transmitting and disclosing personal data, commercial enterprises should abide by certain principles inherent in Kuwait law. In particular, the principles of fairness, transparency, confidentiality and respect for privacy. This means that the collection of personal data should not be fraudulent or illicit and the consent of the individual to such collection, use, transmission or disclosure should be obtained.

Protected data:

See above.

Restrictions on transfer of data offshore:

No specific restriction.

Lebanon

Lebanon does not have general data protection laws. However, there are specific confidentiality provisions relating to: (i) the financial sector; (ii) medical information; (iii) confidential information disclosed to professionals or officials; and (iv) consumers' information.

Applicable legislation:

The financial sector

In Lebanon, the main piece of legislation on privacy is the Banking Secrecy Law of September 3, 1956 (the Banking Secrecy Law) which applies to banks and financial institutions. Article 2 of such law states the following:

"Managers and employees of banking institutions [.....] as well as any person who by virtue of their position or function, have knowledge through any means of the bank's book entries, banking transactions, and correspondence, are bound to absolute secrecy in favour of the bank's clients and may not disclose to anyone, whether a private individual or an administrative, a military or judicial governmental authority, the names of clients, their assets and any matter concerning such clients, except with the written authorisation of the client or his heirs or legatees, or if the client is declared bankrupt, or in the event of a dispute between the client and the bank resulting from banking transactions."

Violation of the Banking Secrecy Law is a criminal offence with offenders facing imprisonment for a period of between three months and one year. The general principle of banking secrecy may be suspended by a decision of the Special Investigating Committee at the Central Bank of Lebanon in relation to cases of money laundering.

Two other laws were enacted in the financial sector in 2011:

- Law No. 160 of 17 August 2011 on Prohibiting Insider Trading made on the Basis of Material Non-public Information (Law 160/2011), and
- Law No. 161 dated 17 August 2011 on Capital Markets (Law 161/2011).

However, these two laws have not been implemented at the time of writing.

Under Article 55 of Law 161/2011, any person who is or has been a part of the Capital Markets Authority, or any company or collective investment scheme operating on the Lebanese capital markets, must keep confidential any information or facts he becomes aware of by virtue of his position or work, and which is related to investors in these markets or any company or entity concerned by such investment.

This confidentiality obligation may not be invoked when requests are addressed to the concerned parties through the Chairman of the Capital Markets Authority Board, either by the Board itself, the Capital Markets Control Unit, the Sanction Committee, the Capital Markets Court or the Criminal Courts.

Deliberate or attempted violation of the confidentiality obligation under Law 161/2011 is sanctioned by imprisonment for a period of between three months and one year.

Law 160/2011 and its implementing Decision No. 6 on Prohibiting Insider Trading made on the Basis of Material Non-public Information on Financial Markets issued by the Capital Markets Authority on 20 November 2013 ("Decision 6/2013") prohibit insider trading made on the basis of material non-public information (Article 2 and subsequent of Law 160/2011 and Article 2 and subsequent of Decision 6/2013).

Violation of this prohibition is sanctioned by imprisonment for a period of between one and three years and by a monetary fine amounting to not less than twice the amount of the profit earned (up to a maximum of ten times such earned profit). The convicted person may also be prohibited from carrying out the profession, whether on a temporary or permanent basis (Article 6 of Law 160/2011). In addition, administrative sanctions may be applied by the Capital Markets Authority on the breaching party (Article 9 of Decision 6/2013).

Medical information

Code of Medical Ethics (Law no. 288 of February 22, 1994) imposes a very strict confidentiality obligation on physicians in favour of patients (Article 7 of the law). A physician who violates such obligation is referred to the Disciplinary Board of the Lebanese Order of Physicians. Sanctions range from a warning to permanent suspension of the physician's licence.

Consumers' information

Under Articles 51 and 58 of the Consumer Protection Code (Law no.659 of 4 February 2005), suppliers must not disclose information provided to them by consumers without the consumer's approval. Such prohibition applies to transactions carried out door-to-door or at a distance whether by telephone, internet or similar means. Suppliers must also take all necessary measures to preserve the confidentiality of such information. The penalty for infringement is a fine of between LBP 30 million and LBP 50 million (equivalent to US$20,000 and US$33,000 respectively).

Protected data:

See above for types of information protected.

Restrictions on transfer of data offshore:

None.

Oman

The data and information technology regulatory authority in Oman is the Information Technology Authority (the ITA). There is no primary data protection or privacy law in Oman.

To a limited extent data protection provisions are set out in various laws issued by Royal Decrees or subordinated legislation. Companies trading in Oman adopt their own data privacy measures which are quite often similar to European standards, but without the enforcement provisions of the supporting legislation.

Applicable legislation:

The basic law, which is in essence the fundamental constitutional law of Oman issued pursuant to Royal Decree No. 101/1996 (as amended) (the Basic Law), provides under Article 27 citizens the right to a private life. It further guarantees citizens confidentiality in all forms of communication by virtue of Article 30 of the Basic Law.

The electronic transactions law issued pursuant to Royal Decree No 69/2008 (as amended) (the Electronic Transactions Law) and the cyber crimes law, issued pursuant to Royal Decree No 12/2011 (as amended) (the Cyber Crimes Law) are the two main pieces of legislation in this area. There are also some provisions relating to confidentiality and protection of personal data in the banking law Royal Decree 112/2000 (as amended) (the Banking Law), circulars of the Central Bank of Oman (the CBO) and the Insurance Regulations issued by the Capital Market Authority (the CMA).

The Electronic Transactions Law, Article 43, deals with the protection of private data. Although this legislation is aimed specifically at e-commerce, it does provide certain safeguards and criminal sanctions against the illegal use of such data.

The most recent law impacting this area is the Cyber Crimes Law. Chapter 2 of the Cyber Crimes Law covers violations of safety, confidentiality of data and systems and some of the penalties for hacking crimes are increased if they involve the misuse of personal data.

Protected data:

Data protection and privacy law has not been developed to European standards in Oman. Therefore companies trading in Oman have taken to adopting their own data privacy measures.

The Cyber Crimes Law increases the penalty for a hacking crime if the data and information is "personal".

Restrictions on transfer of data offshore:

A person transferring data offshore from Oman will be required to ensure that data transferred outside of Oman or to third parties will be subject to data protection requirements as applicable in Oman as a minimum requirement. In addition, the following would also require consideration:

- the nature of the data being transferred;
- the origin of the information;
- purpose and the period for which the data is intended to be transferred;
- the country to which the data is to be transferred, its international obligations and the law in force in that country;
- the relevant rules that are enforceable in that country; and
- the security measures taken to protect the data in that country.

Pakistan

There is no specific data privacy legislation currently in force in Pakistan. Further, as far as we are aware, there are no decided cases in Pakistan on this issue. However, data privacy is to some extent covered in other regulations in Pakistan.

Applicable legislation:

Data privacy would be regulated in Pakistan by:

- the common law of tort and in particular the law relating to breach of confidence; and
- where applicable:

(i) the general laws of contract as reflected in the Pakistan Contract Act 1872 (the Contract Act);

(ii) the Pakistan Telecommunication (Re-organisation) Act 1996 (the Telecommunication Act); and/or

(iii) the Electronic Transactions Ordinance 2002 (the Electronic Transactions Ordinance).

Since the law of torts is not very well developed in Pakistan, the courts have shown a tendency to place reliance on judgments given by courts of England and Wales and other common law countries. Such foreign judgments are not binding on the courts in Pakistan, but they are of persuasive value and have generally been followed. As such, English decisions on the subject prior to the UK Data Protection Act 1998 would be relevant in Pakistan. The English common law of tort (which is usually considered persuasive by the courts in Pakistan) does not recognise invasion of privacy as a free-standing cause of action. Instead, it requires that "privacy" claims must be brought under established common law torts, such as breach of confidence or statutes such as data protection laws. Further, it is now well established that the following three requirements must be satisfied in order to succeed in an action for breach of confidence, namely:

- the information must "have the necessary element of confidence about it" (i.e. it must not be in the public domain);
- the defendant must be under "an obligation of confidence"; and
- the defendant must make "unauthorised use" of the information.

Parties can use the general principles laid down in the Contract Act to contractually agree and collect or disseminate personal information. Privacy of personal information could be ensured by means of contract, any breach of which would entitle a party to rescind the contract and take recourse in the courts to remedy such breach. Database operators can also contract with the individuals from whom they collect data to waive, in writing, any confidentiality requirements pertaining to such data.

Section 31 of the Telecommunication Act provides a penal sanction in the form of a maximum punishment of three years and/or a fine of up to PKR 10 million (approximately US$95,250) against any person who, inter alia:

- prevents or obstructs the transmission or delivery of any intelligence through a telecommunication system or telecommunication service;
- intercepts, acquaints himself with the contents of any intelligence or without authorisation discloses to any person the contents of such intelligence;
- without authorisation deciphers the contents of any message transmitted over a public switched network; or
- without authorisation transmits through a telecommunication system or telecommunication service any intelligence which he knows or has reason to believe to be false, fabricated, indecent or obscene.

Pakistan has enacted the Electronic Transactions Ordinance which, inter alia, provides legal recognition to electronic documents, communications and transactions in electronic form, as alternatives to paper-based methods of communication and storage of information. Sections 36 and 37 of the Electronic Transactions Ordinance provide penal sanctions in the form of a maximum punishment for seven years and/or a fine of PKR 1 million (approximately US$9,525) against any person who:

- without authorisation, gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information; and
- without authorisation alters, modifies, deletes, removes, generates, transmits or stores any information through or in any information system.

Draft laws:

The Electronic Data Protection Act 2005 (the Draft Electronic Data Protection Act) is draft legislation which has been under consideration for a while and although not yet having the force of law should be taken into account. The Draft Electronic Data Protection Act provides, inter alia, that the use, recording, storage, adaptation, blocking, erasure or disclosure of any personal data by means of any information system or other automated means, requires the prior approval of the person to whom such data is related.

The Draft Electronic Data Protection Act under section 7, allows for the collection of local data, (i.e. both personal and corporate data collected within Pakistan for processing within or outside of Pakistan) on the condition that such data should be: collected with due diligence, fairly and lawfully; collected and stored for specified, explicit and lawful purposes and should be adequate and relevant in relation to the purposes for which it is collected; and should be processed in accordance with the rights of the data subject and kept up to date.

Further, section 8 of the Draft Electronic Data Protection Act requires that prior to collection of any personal data, the data subject should be provided with the following information in writing, namely:

- the purposes and means of the processing;
- whether replies to the questions are obligatory or voluntary;
- the possible consequences of failure to reply;
- the recipients or categories of recipients to whom data may be disclosed, and the limits of data dissemination;
- the existence of his rights; and
- the name or trade name, and the address of the data controller and, if designated, of the data processor.

Section 11 of the Draft Electronic Data Protection Act provides that any electronic data which is subject to processing with the prior approval of the data subject, should be stored or processed subject to the conditions that such data is protected, by means of appropriate precautionary measures, against destruction or loss (including accidental loss), unauthorised access, unlawful processing or processing for purposes other than those for which the data was collected. The Draft Electronic Data Protection Act also contemplates the formulation of minimum security standards and the method for the transfer abroad of personal data (including sensitive personal data) collected within Pakistan.

More recently, the government has proposed a draft law by the name of Electronic Documents and Prevention of Cyber Crimes Act 2014 (Draft Cyber Crimes Act), with the aim to consolidate the laws relating to electronic documents and cybercrimes. This law, if enacted, will repeal The Electronic Transactions Ordinance. This Draft Cyber Crimes Act, inter alia, provides for the creation of a Cyber Authority of Pakistan, which shall be responsible for the prevention, suppression, investigation or prosecution of persons involved in committing, abetting, aiding or attempting, cybercrimes through electronic devices. The Draft Cyber Crimes Act also prescribes penalties for such cybercrimes which include fines and/or imprisonment. For example, a person committing a violation of privacy will be punishable with imprisonment of a term not exceeding three years or fine not exceeding PKR 500,000 (approximately US$4,760) or both. While a person who is responsible for possessing, dealing or handling any sensitive personal data in

an electronic device which it owns, controls or operates, and is negligent in implementing and maintaining security practices and procedures, thereby causing wrongful loss or gain to any person, shall be liable to pay compensation to the person so affected. The Draft Cyber Crimes Act also provides legal recognition to electronic documents, communications and transactions in electronic form, as alternatives to paper-based methods of communication and storage of information. Section 65 of the Draft Cyber Crimes Act states that the provisions of the Draft Cyber Crimes Act shall apply notwithstanding the matters being the subject of the Draft Cyber Crimes Act occur outside Pakistan, in so far as they are directly or indirectly connected to, or have an effect on or bearing in relation to persons, information systems or events within Pakistan.

There is no indication as to when these draft laws will be enacted.

Protected data:

The Telecommunication Act provides protection to "intelligence" which has been defined as "any speech sound, data, signal, writing image or video".

The Electronic Transactions Ordinance provides protection to "information systems" which has been defined as "an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information".

The Draft Electronic Data Protection Act provides protection to:

- "foreign data" means both personal and corporate data collected outside Pakistan and sent to Pakistan for processing purpose only;
- "local data" means both personal and corporate data collected within Pakistan for processing within or outside Pakistan;
- "personal data", means any information relating to an individual, identified or identifiable, directly or indirectly by reference to any other information; and
- "sensitive data" means data revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in political parties, trade unions, organisations and associations with a religious, philosophical, political or trade-union, or provide information as to the health or sex life of an individual and financial, or proprietary confidential corporate data.

Under the Draft Cyber Crimes Act, protection is accorded against cybercrimes which include hacking, unauthorised access or interception of any transmission communication or data, identity theft, impersonation, violation of privacy, committing electronic fraud, cyber terrorism, cyber stalking, spamming, spoofing and squatting, and failure to protect data.

Restrictions on transfer of data offshore:

Section 16 of the Draft Electronic Data Protection Act allows for the transfer of local data to any territory outside Pakistan. However, the Draft Electronic Data Protection Act contemplates that such transfer shall be carried out in the manner as may be prescribed in the Rules framed under the Draft Electronic Data Protection Act. As such, under the Draft Electronic Data Protection Act, retention and transmission of documents, records and information within and outside Pakistan appears not to be barred, provided that the information is legally obtained and appropriately secured.

Palestine

There are no special or separate legislative documents in Palestine that deal specifically with data privacy. However, there are several different laws and regulations that contain restrictions on the disclosure of certain confidential information.

Applicable legislation:

The main law in relation to confidential information is the Penal Law No. 16 of 1960 (the Penal Law), which criminalises the disclosure of confidential information. In particular, Article 355 of the Penal Law states that any person who discloses any official confidential information to any unauthorised person (or to any person who is not legally competent to receive such information) may be imprisoned for up to three years. Moreover, the third paragraph of the same Article provides for a similar punishment in respect of any person who receives confidential information in the context of his or her profession and reveals such information without legitimate cause.

The provisions of the Penal Law are of general application, but there are also certain specific sectoral laws that place high emphasis on confidentiality and a duty to protect privileged information in different circumstances. These include:

- Law No. 3 of 1999 regarding the Palestinian Bar Association, which stipulates in Article 28 that any lawyer is under a strict obligation not to disclose any secret information that he has received from his client or obtains in the context of his profession.
- Similar provisions to those imposed on lawyers noted above, can be found under laws regulating doctors and medical professionals (e.g. pharmacists) as well as financial auditors.
- Laws and regulations that govern the functions and duties of financial brokers and custodians (in particular, Securities Law No. 12 of 2004) impose duties on officers of the stock market and brokerage firms to keep confidential any information they receive.
- Banking Law No. 2 of 2002 (as amended) and the newly enacted Banking Law of 2012 provide that all board members and executive officers of any bank are, jointly and severally, liable in exercising their duty to maintain the secrecy of information regarding the clients of the bank.

Protected data:

See above.

Restrictions on transfer of data offshore:

None.

Qatar

Qatar does not have specific laws on data protection. The Qatar Financial Centre (QFC) has a comprehensive legislative regime applicable to companies established in the QFC.

Applicable legislation:

Qatar laws

Law No. 5 of 2005 protecting Trade Secrets (the Trade Secrets Protection Law);

Law No. 16 of 2010 promulgating Electronic Commerce & Transactions (the Electronic Commerce Law); and

Law No. 34 of 2006 concerning Telecommunications (the Telecommunications Law).

QFC

The processing of personal data is regulated by the QFC Data Protection Regulations of 2005 (the Data Protection Regulations). Under these regulations, a data controller (Data Controller) (i.e. any person in the QFC who alone or jointly with others, determines the purposes and means of the Processing of Personal Data, as defined in the Data Protection Regulations) must ensure that the data it processes is (amongst other things) processed fairly, lawfully and securely, and for specified, explicit and legitimate purposes in accordance with the applicable rights of the data subject (Data Subject) (as defined in the Data Protection Regulations).

Protected data:

Qatar laws

Power has been given by the Electronic Commerce Law to the Supreme Council of Information & Communication Technology to establish a framework to protect information and the personal information of the customer of any electronic commerce service provider.

Under the Telecommunications Law, service providers shall be responsible for keeping information and data related to their clients and such clients' communications private and they shall not collect, use, retain or declare any information about their clients unless the clients approve the same.

QFC

Personal data (Personal Data) means any information relating to an identified natural person or an Identifiable Natural Person (as defined in the Data Protection Regulations).

Restrictions on transfer of data offshore:

Qatar laws
None.

QFC
A transfer of Personal Data to a recipient located in a jurisdiction outside the QFC may take place only if an adequate level of protection for that Personal Data is ensured by laws and regulations that are applicable to the recipient. In the event a recipient is not subject to laws and regulations which ensure an adequate level of protection, the Data Controller may not transfer unless (among other things) the QFC Authority (QFCA) has granted a permit for the transfer and the Data Controller applies adequate safeguards with respect to the protection of the Personal Data.

Saudi Arabia

There is no specific law dealing with privacy and personal data in Saudi Arabia. Instead, however, there are provisions contained in various pieces of legislation (and industry circulars) that may apply and should be considered depending on the circumstances.

Applicable legislation:

The most general privacy related legislation is found in the 1992 Basic Law of Government (the Basic Law). Article 40 of the Basic Law provides that: "[t]elegraphic, postal, telephone, and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or listened to except in cases defined by statute."

Part I, Chapter 2 (General Provisions) and Part XIII (Work Inspection) of the Saudi Arabia Labour Law (Labour Law). Article 20 of the Labour law creates a broad prohibition on an employer or an employee "... undertak[ing] any act that infringes upon the freedom of the other or the freedom of other workers or employers to realise any interest or impose a point of view that conflicts with the freedom of work or the jurisdiction of the competent authority in charge of settlement of disputes."

In practice the Basic Law and Labour Law function to provide a degree of transparency in the workplace but protect employees from oppressive intrusions into their personal domains.

Outside of the dynamic between the employer and the employee, the Labour Law also recognises a right of the Government to inspect the workplace for labour violations. Article 198 of the Labour Law grants Government work inspectors the right to:

"(1) [a]ccess any firm that is subject to the provisions of the Labour Law at any time, day or night, without prior notice.

(2) Perform any examination or investigation required to ascertain proper implementation of the Law. [Government work inspectors] may in particular:

(i) Question the employer, his representative or the workers in private or in the presence of witnesses about any matter relating to the implementation of the provisions of the Law.

(ii) Review all books, records and other documents required to be kept pursuant to the provisions of this Law and related decisions, and obtain any copies or extracts therefrom..."

This broad grant of authority provides considerable discretion to Government work inspectors in defining the scope of an inspection and may in practice lead to increased access to personal data and/or intrusions into the private domain of the employer or employee.

The Electronic Crimes Combating Law stipulates that producing, preparing, sending or storing (on the internet or a computer) anything that may harm the general law, religious values, general ethics, privacy or private life carries a maximum term of imprisonment of five years and a maximum fine of SAR 3,000,000.

Under the Law of Printing and Publishing, it is not generally permissible to publish news, stories or pictures associated with the secrets of individuals' private lives.

The banking and insurance sectors both have requirements that information obtained during the course of business must not be disclosed except for official purposes.

The Ministry of Health has issued a "Patient's Bill of Rights" which includes patient privacy provisions.

Protected data:

See above for specific examples.

Restrictions on transfer of data offshore:

Not applicable.

Syria

Syria does not have a general data privacy law. However, there are certain privacy and/or confidentiality rules within specific legislation.

Applicable legislation:

Banking Secrecy Law 30/2010: Pursuant to Article 2 of the Banking Secrecy Law 30/2010 applicable to all financial institutions, information relating to clients, their accounts, assets and transactions is considered secret information. Persons obtaining such information while performing their work or pursuant to their work in relation to the financial institution are prohibited from disclosing such information except to relevant government entities for specific purposes (i.e. central bank supervision, taxation, anti money laundering, etc.). Disclosure, or attempted disclosure, of such information to third parties is punishable by imprisonment for a period ranging from three months to one year, notwithstanding any other sanction or penalty that may apply.

Company Law 29/2011 (Articles 68, 152 & 192) considers any information obtained by directors, managers, employees, public auditors and accountants and any representative of a company while performing their works or due to the nature of their position confidential information, except if such information has been previously made public. It imposes an obligation on such persons to observe the secrecy and non-disclosure of data and information obtained while carrying out their work. Such disclosure will lead to their dismissal and payment of indemnification.

Public Auditors and Accountants Law 33/2009 (Articles 48(11), 86 & 88) obliges public auditors and accountants with secrecy and non-disclosure of data and information they obtained while carrying out their work, to any party whatsoever, except for the competent authorities or subject to a court ruling.

Decision 31/2008 of Syrian Commission on Financial Markets and Securities (Article 7) prohibits any person who has obtained insider information from a company to disclose such information to any third party, except the competent authority or the courts. Partners, directors and concerned employees of the company are held personally liable for the breach of confidential information unless they prove that they were unaware of such breach.

According to Decision 17/2009 of the Damascus Stock Exchange (Article 13) any disclosure of secret undisclosed information made to a third party, other than the competent authority or based on a court ruling or order, will place the disclosing party under legal liability which could lead to imprisonment and/or a financial fine of between 300,000 Syrian pounds and 3,000,000 Syrian pounds.

Protected data:

See above for types of information protected.

Restrictions on transfer of data offshore:

No specific restriction.

United Arab Emirates

The United Arab Emirates (UAE) does not have any specific federal laws on data protection but a number of general and sectoral laws can may have an impact on data processing activities. The economic "freezone" areas of Dubai International Financial Centre (DIFC) and Dubai Healthcare City (DHCC) each have their own comprehensive legislative regime applicable to companies established in those zones, which include data protection regulations. In 2013, Abu Dhabi announced the creation of its own financial free zone, the Abu Dhabi Global Market (ADGM), which is expected to commence operations at the end of 2014. ADGM will also have its own legislation and courts system. No information has yet been published regarding the likely scope of regulations in ADGM and whether this will include a specific data protection law.

Applicable legislation:

UAE federal law

There are no general data privacy provisions under the Civil Code 6 (as defined below), allowing private individuals to seek compensation directly for breaches of their privacy rights. However, certain provisions in various federal laws can impact data processing activity, for example:

- The UAE Constitution of 1971 (the Constitution) provides for freedom of communication "by post, telegraph or other means" and guarantees the right to secrecy of such communications.
- Federal Law No. 5 of 1985 (the Civil Code) provides that a person is liable for acts causing harm generally, which could include harm caused by unauthorised use or publication of the personal or private information of another.
- Federal Law No. 3 of 1987 (the Penal Code) is the primary source of criminal law in the UAE. It sets out offences relating to the publication of matters relating to a person's private or family life, the unauthorised disclosure of secrets entrusted to a person by reason of their profession, craft, circumstance or art and the interception and/or disclosure of correspondence or a telephone conversation without the consent of the relevant individuals. The punishment for these offences can include fines and/or imprisonment.
- Federal Law No. 5 of 2012 (the Cyber Crimes Law) contains certain offences relating to particular types of personal data in an electronic or online context.

Both the Penal Code and the Cyber Crimes Law set out criminal offences and do not directly confer rights upon individuals in relation to the misuse of their data. However, Federal Law No. 35 of 1992, as amended (the Criminal Procedures Law) permits a person who sustains a direct personal injury from a crime to pursue their civil rights before the criminal courts during the criminal proceedings.

There are also provisions in certain sector specific laws and regulations that address privacy rights in particular areas, such as:

- Federal Law No. 8 of 1980 (the Labour Law);
- Federal Law No. 6 of 2010 (the Credit Information Law); and
- Federal Law No. 10 of 2008 (the Medical Liability Law).

DIFC
The processing of personal data by DIFC entities is regulated by DIFC Data Protection Law No.1 of 2007 (the DIFC Data Protection Law), which aligns closely with the EU Data Protection Directive 95/46 EC. It was updated in 2012 with the intention of increasing the transparency, efficiency and effectiveness in the exercise of the DIFC Commissioner of DIFC data protection powers including the introduction of a system of fines to encourage compliance. Under the DIFC Data Protection Law, a "data controller" (i.e. any entity in the DIFC that determines the purposes and means of processing "personal data" (as defined in the DIFC Data Protection Law) must ensure that the personal data it processes is (amongst other things) processed fairly, lawfully and securely, and for specified, explicit and legitimate purposes in accordance with the applicable rights of the "data subject" (as defined in the DIFC Data Protection Law).

DHCC
DHCC Regulation No. 7 of 2008 is the Health Data Protection Regulation (the Health Data Protection Regulation) for entities operating in DHCC. The Health Data Protection Regulation is intended to establish certain principles with respect to collecting, using, disclosing and giving access to "patient health information" (see below).

Protected data:

UAE federal law
Private information in the context of the Penal Code is not clearly defined.

Under the Cyber Crimes Law, a person who gains unauthorised access to a website or IT system and amends, deletes or discloses any data or information is subject to additional penalties if the information is personal. The legislation does not define "personal" in this context, but it is likely to encompass matters relating to a person's private or family life (protected under the Penal Code, as described above).

The Cyber Crimes Law also includes specific offences relating to:

- obtaining, possessing, modifying, destroying or disclosing electronic data relating to medical examinations, medical diagnosis, medical treatment or care or medical records without authorisation;

- unauthorised access to credit or electronic card numbers or data or to bank accounts, numbers or data or any other electronic payment method;
- obtaining without legal right any secret number, code, password or any other means of accessing an IT system;
- unauthorised interception and/or disclosure of communications through an IT network;
- use of a computer network or IT system for the invasion of privacy of another person (except where permitted by law) by eavesdropping, interception, recording or other specified means; and
- use of an IT system for amending or processing a record, photo or scene for the purpose of attacking or invading another person's privacy.

There are sector-specific rules regarding the handling and storage of particular types of data, such as employee information (which must be maintained under the Labour Law), personal credit information (under the Credit Information Law) and patient information (under the Medical Liability Law).

Data controlling entities operating in regulated sectors will be subject to rules, guidance and circulars issued by the relevant regulator in relation to particular types of data (for example, telecommunications service providers have to abide by the UAE Telecommunications Regulatory Authority's Privacy of Consumer Information Policy in relation to any consumer information that they collect).

DIFC

"Personal Data" in the DIFC Data Protection Act means any Data relating to a person. The definition of "Data" was updated in 2012 to align more closely with the European approach and limit the scope of protection to information that is realistically searchable. It is defined as information which is:

- processed by means of equipment operating automatically in response to instructions given for that purpose;
- recorded with the intention that it should be processed by means of such equipment; or
- recorded as part of a Relevant Filing System (as defined) or with the intention that it should form part of a Relevant Filing System.

DHCC

"Patient Health Information" means information about a patient whether spoken, written or in the form of an electronic record, that is created or received by any DHCC licensee and which relates to the physical or mental health or condition of the patient, including the reports from any diagnostic procedures and information related to the payment of services. Such information must identify the patient or there must be a reasonable basis to believe that the information can be used to identify the patient.

Restrictions on transfer of data offshore:

UAE federal law

There are no general restrictions on the transfer of data outside the UAE.

Data controlling entities operating in regulated sectors (such as banking, insurance or telecommunications) will be subject to rules, guidance and circulars issued by the relevant regulator. These rules are subject to change, occasionally at short notice. For example, the Telecommunications Regulatory Authority threatened a ban on BlackBerry services in 2010 for reasons that were reported to have included concerns over the hosting of data outside the country. The Central Bank of the UAE is understood to have concerns in relation to the storage of customer information outside of the UAE, although there is no published Central Bank guidance on the subject.

DIFC

A transfer of Personal Data to a recipient located in a jurisdiction outside the DIFC may take place if an adequate level of protection for that Personal Data is ensured by laws and regulations that are applicable to the recipient. The list of countries that the DIFC deems to offer an "adequate level of protection" is set out on the DIFC's website. If a recipient is not subject to laws and regulations which ensure an adequate level of protection, disclosure of confidential information may still take place, if one of the conditions in Regulation 12 of the DIFC Data Protection Law is satisfied. These conditions include circumstances where the data subject has consented to the transfer, where a permit to authorise the transfer has been granted by the DIFC Data Protection Commissioner or, in certain cases, where the transfer is necessary for the performance of a contract, compliance with legal obligations or to uphold the legitimate interests of the data controller.

DHCC

Patient Health Information may only be transferred to a third party located in a jurisdiction outside DHCC if:

- an adequate level of protection for that Patient Health Information is ensured by the laws and regulations that are applicable to the third party;
- the Health Data Protection Ombudsman, or his delegate, has granted a permit or written authorisation for the transfer and the Data Protection Officer applies adequate safeguards with respect to the protection of the Patient Health Information;
- the patient has authorised the proposed transfer; or
- the transfer is necessary for the ongoing provision of healthcare services to the patient.

Asia Pacific

Australia

Australia has a very developed set of general data privacy principles at the federal (national) level which are broadly consistent with the principles in the EU Data Protection Directive 95/46 EC.

These principles apply to the federal and most state government agencies, the medical sector and the private sector generally (subject to an annual turnover threshold).

Applicable legislation:

Privacy Act 1988 (Cth)
The information in this overview relates to the federal legislation, but a data user may also need to consider state level legislation and guidelines, such as the Privacy and Personal Information Protection Act 1998 (New South Wales).

There are also industry specific rules and codes of practice for banking, medical services, e-commerce and telecommunications.

Protected data:

Information or opinions about a living individual whose identity is apparent or can be reasonably ascertained.

A higher degree of regulation applies to "sensitive information" relating to a person's race, political opinions or association, religious or philosophical belief, trade union membership, sex preference, criminal record, health or genetic information.

Restrictions on transfer of data offshore:

There are restrictions on the transfer of data outside Australia, subject to exemptions. The Australian Privacy Principles 8 address cross-border disclosure of personal information. In addition, following amendments to the federal legislation on 12 March 2014, an Australian entity may be held responsible, in certain circumstances, for any breaches of privacy by an offshore entity to which the Australian entity discloses personal information.

China

The People's Republic of China (PRC) does not have a comprehensive legal framework for data protection. The current legal regime is based on a plethora of laws and regulations in general or as applicable in specific industry sectors.

Applicable legislation:

Privacy rights are generally recognised and protected under the Constitution Law and General Principles of Civil Law in China.

The seventh amendment to the Criminal Law in 2009 makes it a criminal offence for employees of government institutions or private organisations in the financial, telecommunications, transportation, education or medical sectors to sell or otherwise unlawfully provide to third parties personal data of any citizen that has been obtained in the course of performing his duties or services. The amendment to the Tort Liability Law in 2009 creates a private right of action for breach of privacy, although it remains unclear how this will impact on data privacy issues.

The Standing Committee of the National People's Congress issued the Decision on Strengthening the Network Information Protection (the Decision), effective since 28 December 2012. This is the first set of laws at national level specifically regulating online data privacy. Absent a specific definition, any electronic information which could potentially identify an individual or relate to the privacy of citizens is protected under the Decision.

The Information Security Technology Guidelines for Personal Information Protection (the Guidelines) issued by the General Administration of Quality Supervision, Inspection and Quarantine and the Standardisation Administration of the People's Republic of China, in effect since 1 February 2013, impose specific requirements on each stage of collection, processing, transmission and deletion of personal data. The Guidelines specifically prohibit the off-shoring of personal data, unless otherwise explicitly consented or approved by the data subjects, the law or competent authorities. However, since the Guidelines do not technically have the force of law, it remains to be seen how it will be applied in practice.

In addition, the disclosure and transfer of information may potentially fall foul of the Protection of State Secrets Law.

Protected data:

There is no single definition of "personal information" under PRC law. However, separate definitions may exist under industry-specific laws. For example, "personal financial information" protected under the Notice to Urge Banking Financial Institutions to Protect Personal Financial Information issued by the People's Bank of China (PBOC Notice) covers personal identity information, personal property information, personal account information, personal credit information, personal financial transaction information and other personal information of relevant individuals.

Restrictions on transfer of data offshore:

There are no general restrictions on transfer of data offshore. However, industry-specific laws may impose restrictions or prohibitions on international transfer of data, in particular in highly-regulated industries. For example, in the banking and financial institution sector, the PBOC Notice specifically prohibits banks from storing, processing or analysing outside China any protected personal financial data which has been obtained in China, or providing such data to an offshore entity, unless the laws of China or the People's Bank of China provide otherwise.

Hong Kong

Hong Kong has a comprehensive legislative regime that is broadly in keeping with the EU Data Protection Directive 95/46 EC. It regulates how a data user should collect, hold, process or use personal data relating to a data subject.

Applicable legislation:

Personal Data (Privacy) Ordinance

The amendments to the Personal Data (Privacy) Ordinance (the Ordinance) in 2012, have come into effect. The amendments impose increased notification and consent requirements for data users that seek to sell, use or provide to another personal data for direct marketing, and also significant penalties for data users who breach these requirements. The Privacy Commissioner is also empowered to provide legal assistance to aggrieved persons who may institute proceedings to seek compensation. New Guidance Notes published by the Privacy Commissioner have clarified the procedures to be adopted when gathering personal information that may be used for the purpose of direct marketing.

Protected data:

The Ordinance protects information 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 which is in a form in which access or processing of the data is practicable.

Restrictions on transfer of data offshore:

There are controls on transfer onshore in place in the Ordinance, but these have not yet come into effect. The transfer of personal data offshore should be in compliance with the general data privacy principles and the data subject's consent should be obtained, unless one of the exemptions applies. There are also specific controls in place for the offshore transfer of data by financial institutions.

India

In April 2011, India issued the information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the Privacy Rules) pursuant to the Information Technology (Amendment) Act 2008 (the Information Technology Act), which prescribe how personal information may be collected and used by organisations in India.

Applicable legislation:

The Information Technology Act, the Privacy Rules and other relevant rules and regulations.

The Privacy Rules provide detailed provisions relating to protection of data such as: collection and use of personal information; mandatory publication of privacy policy for corporations that collect personal information; technical requirements for security practices and procedures; and disclosure of personal information. These provisions also provide additional specific obligations concerning the treatment of sensitive personal data.

Protected data:

Personal information is defined as any information that relates to an individual, which, either directly or indirectly, in combination with other information available, is capable of identifying such person.

Sensitive personal data is broadly defined as personal information which consists of information relating to: (i) passwords; (ii) financial information such as bank account, credit card, debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sex orientation; (v) medical records and history; (vi) biometric information; or (vii) any detail relating to the above as provided to an organisation, under a lawful contract or otherwise, for providing services or processing.

Restrictions on transfer of data offshore:

Transfer of sensitive personal data outside of India is permitted if the receiving country has the same level of data protection as those provided by the Privacy Rules. The transfer may only be allowed if it is necessary for the performance of an agreement between the organisation and data subject or where the data subject has consented to the transfer.

Indonesia

Indonesia has no laws and regulations specifically covering data privacy. Data privacy is principally regulated by the following legislation:

- **Law No. 11 of 2008 on Electronic Information and Transactions (the EIT Law); and**
- **Government Regulation No. 82 of 2012 on Implementation of Electronic Systems and Transactions (the Regulation).**

As with other local laws and regulations, the EIT Law and the Regulation do not go into great detail. Implementation is often driven by policy, and relies on regulations issued at the ministerial level.

Applicable legislation:

The EIT Law and the Regulation address the collection and use of personal data through electronic media, and essentially mandate the consent of individuals whose data are being collected and used.

Aside from the EIT Law and the Regulation, there are other legislations covering protection of personal data and confidentiality of information, including:

- the Indonesian Criminal Code (the ICC);
- Law No. 39 of 1999 on Human Rights (the Human Rights Law);
- Law No. 23 of 2006 on Demographic Administration (the Demography Law);
- Law No. 36 of 2009 on Health (the Health Law); and
- the banking law and several of its implementing regulations.

On 6 August 2013, Indonesia's Financial Services Authority (Otoritas Jasa Keuangan or OJK) issued Regulation No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector (the Consumer Protection Regulation). The Consumer Protection Regulation protects the confidentiality of consumer data in the financial services sector. It covers data held by banks, insurance companies and other non-bank financial institutions.

Protected data:

Unlike other jurisdictions, Indonesia does not differentiate between personal data and sensitive personal data. The Regulation defines "personal data" as data of an individual which is retained, maintained and secured and of which the integrity and confidentiality are protected.

Restrictions on transfer of data offshore:

Given that Indonesian laws and regulations are often general and that their implementation can be unclear, the prudent course of action is always to obtain the specific consent of the individuals concerned in order to use their data. Under the EIT Law, any person who intentionally and without authority or unlawfully in any manner whatsoever, moves or transfers electronic information and/or electronic documents to unauthorised electronic systems faces imprisonment and/or a fine.

Japan

Japan has a sophisticated and unique data privacy regime. Corporate procedures put in place for compliance with EU data privacy laws may not be suitable for use in Japan.

Applicable legislation:

The Personal Information Protection Law in Japan creates a general data privacy regime for information held by both government and private sector data users.

There is also a series of data privacy guidelines published by different Ministries in Japan which, although they do not technically have the force of law, are generally complied with by data users. Ministry guidelines for data privacy have been published for the telecommunications, financial services, transport and medical sectors.

Protected data:

The Personal Information Protection Law covers information that identifies or may be used to identify a living individual by name, date of birth or other description about an individual.

Restrictions on transfer of data offshore:

No specific prohibitions. However, the disclosure to a third party whether within Japan or offshore must comply with the general data privacy principles and consent should generally be obtained from the data subject unless one of the exemptions applies.

Malaysia

Malaysia has introduced the Personal Data Protection Act 2010 (the Act) which imposes certain obligations on persons who process or instruct the processing of personal data in Malaysia (these persons are known in the Act as "data users"). The Act was given Royal Assent and published in the Gazette in June 2010, and came into effect in November 2013. The Act introduces new obligations where previously data protection was only governed by sector specific laws and common law.

Applicable legislation:

The Act requires data users to adhere to the following seven Personal Data Protection Principles (the Principles) when processing data:

- the General Principle;
- the Notice and Choice Principle;
- the Disclosure Principle;
- the Security Principle;
- the Retention Principle;
- the Data Integrity Principle; and
- the Access Principle.

Failure to adhere to the Principles constitutes an offence under the Act.

The Act also gives individuals the right to take certain actions in relation to their own personal data such as: (i) the right to access and correct the personal data held by data users; (ii) the right to withdraw consent to the processing of the personal data; and (iii) the right to prevent data users from processing personal data for the purpose of direct marketing. Data users are required to respond promptly to any withdrawal of consent or request for access or correction.

The failure of a data user to cease processing personal data in particular would constitute an offence under the Act.

In addition to the above mentioned obligations, certain classes of data users specified by the Minister are required to register with the Personal Data Protection Commission (the Commission).

The Commission is the body tasked with implementing and enforcing the personal data protection laws and approving codes of practice for data users. Officers of the Commission are also given wide powers of investigation under the Act. The Commission is advised by an Advisory Committee and the decisions of the Commission under the Act can be appealed to the Appeal Tribunal.

There is also sector specific law and common law which govern the use and disclosure of confidential information (this may include personal data). Examples of these laws include: the Financial Services Act 2013; the Islamic Financial Services Act 2013; the Labuan Financial Services and Securities Act 2010; the Labuan Islamic Financial Services and Securities Act 2010; and the common law duty of bank confidentiality. Persons who are subject to these laws may also be regulated by bodies other than the Commission with regards to their processing of personal data, such as the Central Bank of Malaysia and the Labuan Financial Services Authority.

Protected data:

Personal data is information in respect of commercial transactions that relates directly or indirectly to the data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user. Sensitive personal data is regulated more closely, but does not include the wide range of sensitive categories used in other countries. "Sensitive personal data" in the Act is currently limited to personal data relating to the individual's health, political opinion, religious belief or criminal record (other categories may be designated by the Minister in the future).

Restrictions on transfer of data offshore:

Generally, the Act does not permit a data user to transfer any personal data out of Malaysia. However, there are exceptions which include:

- where the data user has obtained the individuals' consent to the transfer of their personal data to a place outside of Malaysia;
- where the data user has ensured that the recipient outside Malaysia will process the personal data in a manner which meets the same standards imposed by the Act; and
- where the Minister has specified that the recipient's country is one to which the transfer of personal data is allowed (the Minister has yet to specify any such country at the date of publication).

New Zealand

New Zealand has a comprehensive data privacy law that covers both the public and private sectors and is broadly similar to the EU Data Protection Directive 95/46 EC. New Zealand has been declared by the European Commission as providing an adequate level of protection for personal data transferred from the European Union.

Applicable legislation:

The Privacy Act 1993 (the Privacy Act) regulates the activities of persons who control the collection, holding, processing or use of personal data. Data holders must comply with the 12 information privacy principles set out in the Privacy Act. The Privacy Act gives the individual concerned the right to access and correct their personal information.

The Privacy Act gives the Privacy Commissioner the power to issue codes of practice that become part of the law. The Privacy Commissioner has issued codes in certain sectors including, health, telecommunications and credit reporting industries, and for civil defence and national emergencies.

Protected data:

Information about an identifiable individual. Information that is not protected includes information that is publicly available or used in a form which is not capable of identifying an individual.

Restrictions on transfer of data offshore:

In accordance with amendment legislation passed in September 2010, the Privacy Commissioner may issue a transfer prohibition notice to prevent the transfer of personal information outside of New Zealand. The Privacy Commissioner may issue a transfer prohibition notice on the grounds that:

- information from the organising state has been or will be routed through New Zealand before being transferred to a third state which does not have safeguards comparable to the Privacy Act; and
- the transfer would be likely to contravene the principles on collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.

As at 31 January 2014, the Privacy Commissioner has not issued any transfer prohibition notices.

Philippines

The Philippines has signed into law the Republic Act 10173, also known as the Data Privacy Protection Act of 2012 (the Act). It is a comprehensive data protection law designed to protect individual personal data stored in information and communications systems in both government and private systems. Previously, data protection was subject only to industry specific regulations.

The Philippines has also enacted Republic Act 10175, also known as the Cybercrime Prevention Act of 2012, which is intended to protect and safeguard the integrity of computer and communications systems, networks and databases and the confidentiality, integrity and availability of information and data stored therein, from all forms of misuse, abuse and illegal access by punishing such conduct.

Applicable legislation:

The Act provides guidelines for the "processing" of personal information and prescribes penalties for their violation. It also creates a government body to craft more detailed regulations on data privacy. Under the Act, laws and rules pertaining to processing of personal information that are inconsistent with the Act are also deemed repealed or modified.

Other applicable legislation includes the Electronic Commerce Act and the Guidelines for the Protection of Personal Data in Information and Communications Systems in the Private Sector (issued by the country's trade and industry department).

Protected data:

The Act governs the "processing" of all "personal information" by both natural and juridical persons. "Personal information" refers to any information from which the identity of an individual can be ascertained. "Processing" refers to any operation or set of operations performed upon personal information.

Restrictions on transfer of data offshore:

There are no specific restrictions on transfer of data offshore, but transfer will be subject to general principles of data privacy (i.e. transfer, as a "use" of the data generally requires consent).

Singapore

Personal data in Singapore is protected by common law, sector specific laws and the new Personal Data Protection Act 2012 (the Act) which came into force in January 2013.

Applicable legislation:

The Act will apply concurrently with the existing framework of common law and sector specific laws relating to personal data. The Act does not apply to public sector entities which will be governed by a set of government specific data protection rules and legislation.

The Act consists of two parts, the first being the "Do Not Call Registry" (the DNC Registry) provisions and the second being the data protection rules (the Rules). The Act will come into effect in phases.

Provisions relating to the DNC Registry came into force in January 2014 and the Rules came into force in July 2014.

The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages (such as SMS or MMS), and faxes from organisations.

The Rules govern the collection, use, disclosure and care of personal data and recognises the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

Under the general common law, confidential information may be protected under a duty of confidence. Personal information is also protected under sector-specific laws such as the Banking Act, Statistics Act, the Official Secrets Act and the Statutory Bodies and Government Companies (Protection of Secrecy) Act. The Spam Control Act 2007, Electronic Transactions Act, National Computer Board (Amendment) Act and the Computer Misuse (Amendment) Act provide various regulations for personal information collected, stored or transferred electronically.

Singapore also has a voluntary Model Data Protection Code (the Model Code) for the private sector that is available for adoption by any private organisation that collects personal data. The Model Code imposes practices broadly consistent with the EU Data Protection Directive 95/46 EC.

Protected data:

The Act defines personal data as data, whether true or not, about an individual who can be identified from that data or from that data together with other information to which an organisation has or is likely to have access to.

Restrictions on transfer of data offshore:

The Rules provide that an organisation may transfer personal data to a country or territory outside Singapore only if the transferring organisation has ensured that the recipient organisation will provide a standard of protection to the personal data that is comparable to the level of protection prescribed by the Rules.

South Korea

South Korea has recently enacted a comprehensive law on data privacy based upon the EU Data Protection Directive 95/46 EC, OECD Guidelines and the APEC Privacy Framework.

Applicable legislation:

The Personal Information Protection Act, which came into force on 30 September 2011, is the general law governing the protection of the privacy of personal information and regulating the collection, handling and use of personal information. Other legislation such as the Act on Usage and Protection of Credit Information and the Act on Promotion of Usage of Information Telecommunications Networks and Protection of Information may continue to apply to information collected in specific areas.

Protected data:

The Personal Information Protection Act defines personal information as information that pertains to a living person, including their full name, resident registration number and images etc. by which the individual in question can be identified (including information by which the individual in question cannot be identified but can be identified through simple combination with other information).

Restrictions on transfer of data offshore:

Consent for the transfer of data outside South Korea is required to be obtained prior to transfer, in accordance with Article 17(3) of the Personal Information Protection Act.

Taiwan

On October 1 2012, Taiwan put into effect a comprehensive amendment to the 1995 Computer-Processed Personal Data Protection Act, now entitled the Personal Data Protection Act (the Act). The Act provides comprehensive regulation of the collection, processing and use of personal data for all data users. The previous legislation only covered public agencies and specific industry sectors, and only in relation to the processing of data in electronic form.

Applicable legislation:

Personal Data Protection Act

Protected data:

Personal data is defined in the Act as a natural person's name, date of birth, national identification number, passport number, special features, fingerprints, marriage, family, education, occupation, medical records, medical history, generic information, sex life, health examinations, criminal records, contact information, financial status, social activities and other data which is sufficient to, directly or indirectly, identify that person.

Restrictions on transfer of data offshore:

International transmission of personal data within the scope of specific purposes for which data are collected is currently permitted.

Thailand

There is no comprehensive data protection law in Thailand. However, legislative and administrative regulations are in place which impose data protection regulations in certain areas such as credit information.

Applicable legislation:

Legislation which incorporates data protection provisions, include:

- the Official Information Act;
- the Credit Information Business Act;
- the Bank of Thailand Notification No.SorNorSor 16/2552 re: Designation of Criteria, Procedures and Conditions of the Operation of Credit Card Business by Commercial Banks; and
- a draft Personal Data Protection Bill was proposed in 2013, but there is currently no timetable for its enactment.

Protected data:

The Official Information Act broadly defines personal information, but only as relates to Thai nationals or residents and to activities of State agencies in respect of that information. The Credit Information Business Act, as its name implies, covers the use of personal information in a very specific industry context.

Restrictions on transfer of data offshore:

None.

Vietnam

Vietnam has no general data protection law. However, personal data may be protected by the civil law.

Applicable legislation:

Vietnam does not have a comprehensive data privacy protection law. Instead general confidentiality protection provisions for personal data are included in the Civil Code. In relation to electronic personal data, regulation is provided by the Law of Information Technology and Law on Electronic Transactions which deal with the processing of electronic personal data.

Information obtained by businesses from consumers is protected by the Law on Protection of Consumers' Rights. The nature of the protection is similar in each case, although there are slight differences in wording.

Protected data:

The Civil Code protects information relating to the private life of a person. This is a general provision and it applies in all circumstances.

The Law on Information Technology protects information on "personal information". It says that such information must only be used for a "proper purpose", although there is no description of what would constitute such a purpose.

The Law on Electronic Transactions protects private information which has been used in an electronic transaction.

Neither the Civil Code nor the Law on Electronic Transactions, define the scope of personal information protected by those laws. The Law on Information Technology and its guiding decrees provide that "Personal Information" includes full name, date of birth, profession, title, contact address, e-mail address, telephone number, ID number, passport number and other information defined by law. "Information belonging to Personal Secrets" includes medical records, tax payment dossiers, social insurance card numbers, credit card numbers and other personal secrets.

The Law on Protection of Consumers' Rights protects "information about consumers", which is not defined within the law.

Restrictions on transfer of data offshore:

In general terms, there are no restrictions. However, if the information is contained in accounting records of a Vietnamese company or other enterprise, there is a requirement for the accounting records to remain in Vietnam for the relevant statutory period.

Contacts

Contacts

If you would like further information, please contact:

Mike Rebeiro
Global head of technology and innovation, London
Norton Rose Fulbright LLP
Tel +44 20 7444 2565
mike.rebeiro@nortonrosefulbright.com

Asia Pacific

Nick Abrahams
Partner, Sydney
Norton Rose Fulbright Australia
Tel +61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

Stella Cramer
Partner, Singapore
Norton Rose Fulbright (Asia) LLP
Tel +65 6309 5349
stella.cramer@nortonrosefulbright.com

Justin Davidson
Partner, Hong Kong
Norton Rose Fulbright Hong Kong
Tel +852 3405 2426
justin.davidson@nortonrosefulbright.com

Barbara Li
Partner, Beijing
Norton Rose Fulbright LLP
Tel +86 10 6535 3130
barbara.li@nortonrosefulbright.com

Michael Park
Partner, Melbourne
Norton Rose Fulbright Australia
Tel +61 3 8686 6499
michael.park@nortonrosefulbright.com

Middle East and Africa

Rohan Isaacs
Director, Johannesburg
Norton Rose Fulbright South Africa Inc
Tel +27 11 685 8871
rohan.isaacs@nortonrosefulbright.com

Gabriel Meyer
Director, Johannesburg
Norton Rose Fulbright South Africa Inc
Tel +27 11 685 8858
gabriel.meyer@nortonrosefulbright.com

Dino Wilkinson
Partner, Abu Dhabi
Norton Rose Fulbright (Middle East) LLP
Tel +971 2 615 1727
dino.wilkinson@nortonrosefulbright.com

Nerushka Deosaran
Associate, Johannesburg
Norton Rose Fulbright South Africa Inc
Tel +27 11 685 8691
nerushka.deosaran@nortonrosefulbright.com

Europe

Jonathan Ball
Partner, London
Norton Rose Fulbright LLP
Tel +44 20 7444 5560
jonathan.ball@nortonrosefulbright.com

Marcus Evans
Partner, London
Norton Rose Fulbright LLP
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Marc d'Haultfoeuille
Partner, Paris
Norton Rose Fulbright LLP
Tel +331 56 59 5373
marc.d'haultfoeuille@nortonrosefulbright.com

Mike Knapper
Partner, London
Norton Rose Fulbright LLP
Tel +44 20 7444 3998
mike.knapper@nortonrosefulbright.com

Nadège Martin
Of Counsel, Paris
Norton Rose Fulbright LLP
Tel +33 1 56 59 5374
nadege.martin@nortonrosefulbright.com

Floortje Nagelkerke
Senior Associate, Amsterdam
Norton Rose Fulbright LLP
Tel +31 20 462 9426
floortje.nagelkerke@nortonrosefulbright.com

Jamie Nowak
Partner, Munich
Norton Rose Fulbright LLP
Tel +49 89 212148 422
jamie.nowak@nortonrosefulbright.com

Malgorzata Patocka
Of Counsel, Warsaw
Norton Rose Fulbright Piotr Strawa and Partners, Limited Partnership
Tel +48 22 581 4920
malgorzata.patocka@nortonrosefulbright.com

Christoph Ritzer
Of Counsel, Frankfurt
Norton Rose Fulbright LLP
Tel +49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

Vera Shaftan
Senior Associate, Moscow
Norton Rose Fulbright (Central Europe) LLP
Tel +7 499 924 5144
vera.shaftan@nortonrosefulbright.com

Christoph Zieger
Senior Associate, Munich
Norton Rose Fulbright LLP
Tel +49 89 212148 423
christoph.zieger@nortonrosefulbright.com

North America

Christine A Carron
Partner, Montréal
Norton Rose Fulbright Canada LLP
Tel +1 514 847 4404
christine.carron@nortonrosefulbright.com

Martha A Healey
Partner, Ottawa
Norton Rose Fulbright Canada LLP
Tel +1 613 780 8638
martha.healey@nortonrosefulbright.com

David Kessler
Partner, New York
Norton Rose Fulbright US LLP
Tel +1 212 318 3382
david.kessler@nortonrosefulbright.com

David Navetta
Partner, Denver
Norton Rose Fulbright US LLP
Tel +1 303 801 2732
david.navetta@nortonrosefulbright.com

Sue Ross
Sr. Counsel, New York
Norton Rose Fulbright US LLP
Tel +1 212 318 3280
susan.ross@nortonrosefulbright.com

Boris Segalis
Partner, New York
Norton Rose Fulbright US LLP
Tel +1 212 318 3105
boris.segalis@nortonrosefulbright.com

Stephen Whitney
Of Counsel, Toronto
Norton Rose Fulbright Canada LLP
Tel +1 416.216.2435
stephen.whitney@nortonrosefulbright.com

Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's pre-eminent corporations and financial institutions with a full business law service. We have more than 3800 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

More than 50 locations, including Houston, New York, London, Toronto, Hong Kong, Singapore, Sydney, Johannesburg, Dubai.

Attorney advertising

NORTON ROSE FULBRIGHT

Law around the world
nortonrosefulbright.com