Data protected.

Linklaters

A global report on the status of data protection laws in 2013.

Europe looking beyond its borders.

Welcome to the 2013 edition of Data Protected. Originally launched in 2004 to celebrate the accession of ten new Member States to the European Union, the report is now in its seventh edition and covers 47 jurisdictions around the world.

This edition reflects the increasing importance of data privacy laws in Asia and contains new chapters for the People's Republic of China, Indonesia and Vietnam. It was prepared in association with Allens with whom Linklaters has entered into a new integrated alliance.

The report shows data privacy has an increasingly international dimension greatly influenced by the adoption of the *Data Protection Directive* in the mid-90s. As negotiations over its replacement by the General Data Protection Regulation reach a critical point, the European Union can no longer focus inward creating ever stricter requirements. Instead, a global consensus must be built on data privacy by taking a more balanced approach, recognising the issues raised by "Big Data" (a topic considered in the feature article to this edition) and the fact that modern technology and the internet makes national boundaries increasingly irrelevant. A global world needs a global approach to privacy.

This report only considers issues arising out of the *Data Protection Directive* and the *Privacy and Electronic Communications Directive* as they currently stand, and similar national legislation outside of the European Union. Its purpose is not to provide legal advice or exhaustive information but rather to create awareness of the main rules. Needless to say, each contributing law firm is responsible for the contents of its own section. Should you have any questions in connection with the issues raised or if specific advice is needed, please consult one of the lawyers referred to in the contact list at the end of this report.

Tanguy Van Overstraeten
Partner
Global Head of Privacy and Data Protection
Linklaters LLP
March 2013

Michael Pattison
Partner
Technology, Media & Telecommunications
Allens
March 2013

Contents.

Is “Big Data” creepy?

Is "Big Data" creepy?

The ever growing volumes of electronic data, or "Big Data", present threats and opportunities for organisations as they grapple with the cost of managing that data and explore different ways to analyse, exploit and monetise the information contained within it.

Similarly, Big Data is a threat and opportunity for individuals. On the one hand, most individuals now have instant access to vast amounts of information which provides a wide range of benefits including spurring innovation, communication and freedom of expression. On the other hand, these new pools of data also include information about individuals and the use of Big Data tools to combine and analyse that information could infringe their privacy on a significant scale.

Big Data therefore provides a useful focus for many of the issues currently facing the privacy community and might suggest the need for more, or at least, tighter regulation. However, when the various elements of Big Data are deconstructed – collection, combination, analysis and use – it appears that the current privacy framework addresses most concerns and provides a sensible balance between the risks and benefits of Big Data. In fact, the more compelling case is for less regulation, particularly in relation to unstructured electronic data which is predominantly responsible for the growth of Big Data.

What do we mean by Big Data?

Much of the debate about Big Data has been driven by size. It's clear that huge amounts of data are now being processed with the standard unit of "Big Data" moving from the terabyte, to the petabyte, to the exabyte. To give a sense of scale, Berkley University in California estimated that every word ever spoken by a human being could be stored in five exabytes. However, internet traffic this year alone is estimated to exceed 650 exabytes.

Impressive as these figures are, a vast amount of electronic data is of little use in itself. An important part of the Big Data concept is therefore the new technologies being used to extract meaningful information from that data. Many of the challenges here arise from not only the sheer size of these new data sets but the desire to combine data from multiple different sources in multiple different systems.

Big Data is also characterised by a change in the nature of data held by organisations. Traditionally, data would be stored in a highly structured format to maximise its informational content. For example, a relational database has a set number of fields, each of which will contain a specific type of data in a specific format. This structure would make it easy to process and manipulate by applying simple deterministic rules to that data.

However, current data volumes are not being driven by traditional structured data but instead by an explosion in unstructured or semi-structured data. The majority of the 650 exabytes passing through the internet this year is not tightly structured databases but instead videos, pictures, tweets, emails and the like. From a machine perspective, there are only limited tools (such as facial or voice recognition) that can analyse this data, meaning it is very hard to extract meaningful information. To give an example, a YouTube video of the Harlem Shake may be many megabytes in size but much of it is just noise to a machine.

So a lot of data does not necessarily provide a lot of useful information. Whilst organisations will continue to refine the techniques used to extract useful information from this explosion of unstructured information, these tools are likely to be limited for the immediate future, as is the ability of organisations to apply automated, context-specific decisions about that data. This distinction is important when considering how to regulate Big Data.

What does the public think about Big Data?

Each stage of the Big Data lifecycle – collection, combination, analysis and use – has changed in recent years in a way that could present serious risks to individual privacy. We consider why this is the case below.

What information are they collecting?

The starting point is the collection of information about individuals. Our digital footprint means we are being tracked and monitored more closely than ever before and examples of this electronic breadcrumb trail include:

- *Electronic communications* - Electronic communications such as emails, social network messages and postings, profiles and updates are now an important, and often permanent, means of communications.

- *Internet tracking* - Similarly, cookies, search term analysis and other technology allow organisations to build up detailed profiles of individuals' internet usage habits which can provide significant insights into their life and interests.

- *Financial information* - As cash purchases become less common, more payments are made electronically using a payment card, emoney or similar. Each electronic purchase leaves a record about that individual.

- *Location information* - Modern technology allows an individual's location to be tracked and monitored, most commonly via smartphones or vehicle tracking.

- *Electronic record keeping* - Very few records are now kept in hard copy format meaning more and more information is now moving to an electronic medium.

- *RFID* - The use of RFID technology is increasing, for example through, electronic ticketing such as the Octopus smart card system which caused a serious privacy incident in Hong Kong after it was revealed that customer information was being sold to third parties.

- *CCTV surveillance* - There has been a huge growth in the use of CCTV camera surveillance, both in the public and private sector, with those systems now often being networked and possibly connected to other systems, for example, automated number plate recognition systems used to spot stolen or uninsured cars.

These changes are an irreversible consequence of a move to an electronic world. Individuals are no more likely to give up using social networks than organisations are likely to move back to hard copy record keeping. We live in a world of Big Data and some of that data is about us.

Are they combining that information?

Whilst the mere collection of this information can be intrusive, the privacy risks are multiplied when multiple pools of data are combined. However, combining data from different sources is one of the central aims of Big Data analysis.

One prominent example is Google. In March 2012, Google amended its privacy policy to allow information from its many services (including its search engine, YouTube usage and mapping service) to be combined to help Google build a more detailed profile of its users and thus provide more targeted adverts. The combination of information in this way has generated a swift response from privacy regulators and in February this year the CNIL threatened repressive action if Google did not address some of the compliance issues raised by combining data in this manner. However, even Google understands that there are limits. Its technology could be used to build a facial recognition database capable of searching the internet for someone's image but the idea has been rejected by its Chief Executive, Eric Schmidt, as "crossing the creepy line".

New forms of Big Data combination are also being used by Governments. For example, the UK Government has implemented new information technology techniques to combine its social security and tax records with bank account and credit reference reports to detect benefit theft, tax evasion and organised crime.

What does that data tell them about me?

Perhaps core to many of these privacy concerns is the extent to which this data can be combined to generate meaningful information about an individual – to what extent does Big Data really give an insight into that individual's life?

There are numerous examples of data mining in practice, particularly in relation to traditional structured datasets such as supermarket loyalty schemes. Perhaps the best example is the US Target Superstore which analysed its customers' purchasing behaviour to, amongst other things, identify customers in the early stages of pregnancy. This information is extremely valuable as it allows targeted advertising at a critical point in that customer's life when their behaviour is in flux and new habits are formed. Target's analysis of this information not only demonstrates how useful this information can be to an organisation but also the potential privacy risks to an individual. In at least one case, a customer's pregnancy was revealed to her other family members through targeted advertising containing pregnancy-related products.

More interesting questions arise over the analysis of unstructured data and the extent to which it can provide useful information. For example, some advertising billboards are now using facial recognition technology to estimate a visitor's gender and age to tailor adverts for that particular visitor. Similarly, Google's Gmail service scans emails to identify keywords and deliver targeted adverts. Whilst this appears to be a fairly rudimentary analysis, it is easy to envisage more sophisticated techniques being developed. For example, analysing photos to see if someone had put on weight or someone's voice patterns to determine their mood.

As more and more data is analysed, the greater the potential insights into individual behaviour but also the greater is the potential for this information to be wrong. Some of these inaccuracies might arise from incorrectly crossing traditional databases. Some will arise from the fact unstructured data is hard to analyse and require statistical and probabilistic tools that are not prone to providing definitive answers.

Finally, Big Data analysis will not always be used to provide information about particular individuals and in many cases will use anonymised data or produce anonymised outputs. This is clearly beneficial from a privacy perspective though, perhaps ironically, the world of Big Data makes true anonymisation harder and harder to achieve as it becomes easier to combine and analyse that so-called anonymised data to re-identify individuals.

How is that information being used?

So what is the end point of this process? How will Big Data affect me in practice? One of the most obvious uses of Big Data is marketing but it is used in a wide range of other contexts, including national security, credit scoring and detecting benefit fraud or tax evasion. As Big Data techniques mature, new uses are likely to arise.

Whilst some of these uses are likely to have minimal implications for an individual, others are potentially more significant. This means it is particularly important to ensure that the analysis is providing the right result or that suitable safeguards are in place to protect individuals particularly where there is limited assurance about the accuracy of any Big Data analysis.

The regulatory response

The advent of Big Data gives rise to a number of serious concerns. In many jurisdictions these are directly addressed through regulation. The question is whether that privacy regulation provides adequate protection for individuals whilst also recognising the many benefits of Big Data to society at large and the burdens it places on businesses.

Do data protection laws provide adequate protection for individuals against the use of Big Data?

The core of most data protection laws is a set of generic data protection principles. These principles have been drafted in a technology neutral manner and appear to largely meet many of the concerns raised by Big Data. For example, most data protection laws, including the *Data Protection Directive*, contain the following principles:

- *Notice* – Individuals must normally be told about any processing of their personal information. This provides individuals with an understanding of who is collecting their information and why, and may allow them to exercise some control over its use.

- *Choice and legitimate purpose* – Personal information can only generally be used for certain specified situations, such as where the individual has given consent or where required by law. These purpose limitations generally apply right across the Big Data lifecycle to the collection, combination, analysis and use of that information (though in some jurisdictions each stage is subject to different conditions). This means that every stage of the process is regulated and must be justified, thus reducing the opportunity to misuse that data. Equally, choice may arise where individuals are given control over subsequent use of their information, for example through specific opt-outs.

- *Restrictions on further use* – Personal information processed for one purpose cannot generally be used for other incompatible purposes. This helps to counter the concern that personal information collected for one particular purpose will not be sucked up as part of Big Data analysis for a completely different purpose. It also creates a significant barrier against a Big Data surveillance society in which individuals are subject to omnipresent surveillance.

- *Accuracy* – Personal information must generally be accurate. This principle will help to ensure proper safeguards are in place where there is limited assurance about Big Data analysis or even prevent that analysis being conducted in the first place.

- *Retention* – Personal information must not be excessive or kept for longer than necessary. This helps to prevent the accumulation of Big Data and the risk of historic or out-of-date data being analysed.

However, these generic principles might not always be sufficiently clear or targeted, so they are typically supplemented by more specific rules. These act as a further constraint on the misuse of Big Data:

- *Particular types of data* – Certain types of personal information are given additional protection because of the additional risk that they could be used to infringe an individual's privacy. For example, in Europe it is only possible to process sensitive personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life) in certain limited circumstances.

- *Additional controls on collection* – There are specific controls on the collection of certain information. For example, in the European Union it is necessary to gain consent to use certain cookies and there are strict controls on any subsequent use of traffic or location data.

- *Additional controls on use* – Recognising that certain uses of personal information are a particular concern or annoyance to individuals, they are normally granted specific additional rights, for example, many jurisdictions with data protection laws provide individuals with the right to object to various forms of direct marketing (such as Singapore's recently introduced Do Not Call Register which restricts telephone marketing).

- *Automated decision making* – The use of automated processes to make significant decisions about individuals is also generally subject to controls. These controls are likely to mean that appropriate checks and balances will be in place when decisions are based on Big Data.

Put together, these principles provide a fairly comprehensive package of protection for individuals. Big Data certainly *could* be creepy but in practice its use seems to be largely in accordance with social norms and there is little evidence of obvious gaps in its regulation.

Certainly, where Big Data has been used in potentially infringing way, there has been a swift regulatory response as evidenced by the continuing enforcement action by European regulators against Google for seeking to consolidate user data from its different services or the US Federal Trade Commission's action against Facebook for misleading customers as to whether their information would be made public. In the UK, the Information Commissioner recently prohibited the mandatory installation of video and audio recording equipment in taxis on the basis it would be a disproportionate privacy infringement. In many cases, this involves a somewhat subjective balancing exercise between utility, privacy, proportionality and choice and not everyone would necessarily come to the same conclusion. However, privacy law does seem to provide the appropriate framework for such judgments to be made.

Do data protection laws place appropriate burdens on businesses using Big Data?

The flip side of this question is whether the regulatory burdens placed on businesses are appropriate. Do they allow innovation and reflect the many benefits Big Data can provide?

The position here is less clear and for many businesses reconciling traditional data protection laws with the new world of Big Data is a challenge. This is largely because data protection laws originate out of a world of structured data in which there are distinct pools of data. Each of those pools has a defined purpose and each item of data in that pool has a structure. It is therefore relatively simple to ensure compliance through both a macro-level review of the overall pool of data (for example, to assess if it is being used for a proper purpose) and automatic micro-level application of rules to individual items of data (for example, automatically deleting old data).

For unstructured data, the position is more difficult. The often chaotic mixture of information in emails, photos or videos makes it very difficult to make any sensible macro-level assessment about that data, or to carry out any automated micro-level review of that data. For example, emails may contain information about business transactions, personal communications or resumes, so it is difficult to create a sensible list of purposes for which that data is processed. Equally, each individual email will contain different personal information, and so becomes redundant on a particular date. In some cases, it may be difficult to come to any clear conclusion at all.

For example, consider a video of the Harlem Shake on YouTube – for what purposes is it processed? Entertainment? When is it no longer needed for that purpose? These issues were directly addressed by the Italian Appeals Court when it overturned the convictions of three Google employees for allegedly violating privacy laws. The Court upheld Google's role as an intermediary and found that, amongst other things, Google could not be expected to pro-actively police the content of the videos it hosts, stating : "*it is patently clear that any assessment of the purpose of an image contained in a video, capable of ascertaining whether or not a piece of data is sensitive, implies a semantic, variable judgement which can certainly not be delegated to an IT process*".

These issues have wider resonance. Whilst most organisations want to ensure they comply with the law in full, they simply have too much data, and in particular too much unstructured data, to be able to make any sensible "bottom up" assessment of whether it all complies with the various data protection principles and other requirements of data protection law. Instead,

much is done through approximation and prioritisation. Big Data is creating a credibility gap between the formal expectations of data protection laws and the implementation of those laws in practice.

How will this change under the proposed Regulation?

The current revision to Europe's data protection laws would have provided a good opportunity to re-assess the current approach and undertake the, no doubt, very challenging exercise of trying to develop a new structure that continues to protect individual's privacy but bridges the gap between law and practice.

However, the European Commission proposed General Data Protection Regulation, issued in January 2012, largely retains the fundamental structure, definitions and principles of the earlier Directive. Instead, it tightens many aspects of the previous regime, imposing additional procedural obligations and strengthening enforcement and sanction mechanisms. This overall approach has been followed in subsequent developments, such as the draft report by Jan-Philipp Albrecht, rapporteur for the Civil Liberties, Justice and Home Affairs Committee (LIBE) of the European Parliament.

The combined effect of these proposals could significantly reduce the use and exploitation of Big Data. Some of the more important aspects include:

- *Profiling* – Both the Commission's and LIBE's proposals contain restrictions on profiling. LIBE's proposal greatly widened the definition of profiling, to include automated processing intended to predict an individual's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. The LIBE proposal also only allows profiling to take place with consent (which will be hard to obtain) or in certain other limited circumstances. The combined effect of this change would be to greatly limit the use of Big Data on information about individuals.

- *Prescription* – The proposals would require detailed documentation to be created. Under the LIBE proposal this documentation would have to include details of the categories of personal data processed, the purpose for which personal data is processed, explanation for any reliance on the legitimate interests condition, details of all recipients of personal data. As previous discussed, in a world of Big Data, and particularly unstructured Big Data, it is difficult to accurately and completely identify all such processing. Nor is it clear what the purpose of this documentation would be.

- *Expanded definition of personal data* – The LIBE proposal also expands the definition of personal data and, accordingly, the scope of activities subject to data protection regulation and the restrictions on profiling. For example, personal data would include any unique identifier that could be used to single out a natural person, such as cookies.

Conclusions

The growth of Big Data presents a number of challenges and requires a careful balance between the threats and opportunities it presents to individuals and businesses alike.

Its debatable if the proposed Regulation strikes the right balance. Those changes, taken together with the very significant increase in sanctions for breach, are likely to significantly curtail the use of Big Data, which would be unfortunate. Firstly, there is limited evidence of the need for this additional protection or of widespread misuse of Big Data under the current framework. Secondly, it is likely to have a disproportionate effect on European businesses (though the proposals do extend the Regulation to some business based outside of the EEA). Finally, these limitations could inhibit innovation and deny society the benefits of better understanding the data it holds.

Richard Cumbley
Partner
Technology, Media & Telecommunications
Linklaters LLP
March 2013

Peter Church
Solicitor
Technology, Media & Telecommunications
Linklaters LLP
March 2013

Country overviews.

Argentina

Contributed by Allende & Brea

General | Data Protection Laws

National Legislation

General data protection laws

The Data Protection Act of Argentina, Law 25,326 (the "**DPA**").

Entry into force

The DPA entered into force on November 2, 2000.

National Regulatory Authority

Details of the competent national regulatory authority

Dirección Nacional De Protección De Datos Personales (the "**Directorate**")
Sarmiento 1118 – 5th Floor
Ciudad Autónoma de Buenos Aires
C1041AAX

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

Notification or registration scheme and timing

Any personal database must be registered and the registration must be renewed annually. Registration requires the following information: (i) the name and domicile of the person in charge of that database; (ii) the characteristics and purpose of the database; (iii) the nature of the personal data contained in each file; (iv) the method of collecting and updating the data; (v) the recipients to whom such data may be transmitted; (vi) the manner in which the registered information can be interrelated; (vii) security measures; (viii) data retention period; and (ix) means for individuals to access, correct and update their data.

It is not possible to file a registration electronically. Filing has to be done by lodging hard copies with the Directorate.

Exemptions

Private persons holding personal databases for exclusively personal uses are exempt from registration.

Appointment of a data protection officer

There is no obligation to appoint a data protection officer under the DPA. However, the auditing regulation 5/2008 contains matters relating to data protection and security and requires a specific person to be designated to deal with those issues.

Personal Data

What is personal data?

The DPA defines personal data as "information of any kind referring to certain or ascertainable physical persons or legal entities". The person to whom the personal data relates is known as a "**data owner**".

Is information about legal entities personal data?

Yes.

What are the rules for processing personal data?

The processing of personal data generally requires express consent from the *data owner* which must be accompanied by appropriate information, in a prominent and express manner, explaining the nature of consent sought.

However, consent to processing is not required where the data: (i) comes from a public source; (ii) is collected for the functions of the State; (iii) is collected under a legal duty; (iv) consist of lists limited to name, national identity card number, tax or social security identification, occupation, date of birth, and domicile; (v) arises from a contractual relationship; (vi) arises from a scientific relationship; or (vii) refers to the transactions performed by financial entities, and arises from the information received from their customers in accordance with the provisions of bank secrecy laws.

Additional restrictions apply to the disclosure of personal data. This is generally only permitted where it is in the legitimate interests of the database owner and the *data owner* has consented. This consent can be revoked. However, consent to the disclosure of personal data is not required where: (i) disclosure is provided for by law; (ii) one of the general data processing conditions (set out above) applies; (iii) the disclosure is directly between governmental agencies;

(iv) the disclosure is for public health reasons and appropriate measures are used to hide the identity of individuals; or (v) the information is anonymised so individuals are not identifiable.

The recipient of the personal data will be subject to the same obligations as the person disclosing them and both parties are jointly and severally liable for any subsequent use.

Are there any formalities to obtain consent to process personal data?

Consent must be express and informed. It should be in writing or similar form depending on the circumstances. The DPA does not require any formality to obtain consent to process personal data. Moreover, the DPA permits obtaining consent online by clicking an appropriate icon, without the existence of any written form.

Sensitive Personal Data

What is sensitive personal data?

Sensitive personal data includes all the *standard types of sensitive personal data*. However, there is some debate about whether this is an exclusive definition and whether, for example, it might also cover information that could be used for discriminatory purposes even though, on its face, it is not discriminatory (e.g. an address or zip code from a low income neighbourhood).

Are there additional rules for processing sensitive personal data?

No person can be compelled to provide sensitive personal data.

Sensitive personal data can only be processed: (i) where there are circumstances of general interest authorised by law; or (ii) for statistical or scientific purposes provided *data owners* cannot be identified from that information.

The creation of personal databases that directly or indirectly reveal sensitive personal data is prohibited. However, the Catholic Church, religious associations, and political parties and trade unions shall be entitled to keep a register of their members.

Data referring to criminal offences can be processed only by competent public authorities for purposes established by law.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be express and informed. It should be in writing or similar form depending on the circumstances.

Scope of Application

What is the territorial scope of application?

The DPA applies in the territory of Argentina and to any processing of personal data on the Internet.

Who is subject to data protection legislation?

The DPA applies to owners of databases of personal data ("**data users**"), a concept similar to that of *data controller*. The DPA does not also have the concept of *data processor*.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to "**personal databases**". These include any data file, register, database, data bank or organised set of personal data which is subject to processing, either electronically or otherwise, regardless of the mode of collection, storage, organisation or access.

Rights of Data Subjects

Compensation

The DPA does not specifically provide for compensation. However, compensation may be available under general principles of tort law.

Fair processing information

Whenever personal data is requested, the *data owner* must get express, clear and prior notification of: (i) the purpose for which the data shall be processed; (ii) the recipients or classes of recipients; (iii) the existence of the relevant personal database and the owner of that database; (iv) whether the provision of information is compulsory or discretionary; (v) the consequences of providing or refusing to provide data; and (vi) the *data owner's* right of data access, rectification and suppression.

Rights to access information

Data owners are entitled to access their personal data where it is included in a public database, or in a private database intended for the provision of reports. Requests can be made free of charge and at six-monthly intervals unless there is a

legitimate reason for more frequent access. The requested information must be provided within 10 calendar days. Where the personal data relates to a deceased person, their heirs shall be entitled to exercise this right on behalf of the estate.

The information must be provided clearly with an explanation of any codes or terms used in language that can be understood by a citizen with an average level of education. A full copy of the information about that *data owner* must be provided, even if the request only refers to one item of personal data.

The information may be provided in writing or by electronic, telephonic, visual or other means adequate to communicate that information to the *data owner*.

Objection to direct marketing

Personal databases may be created for direct marketing purposes where the personal data within them: (i) was publicly available; (ii) was provided by the *data owners*; or (iii) takes place with the *data owners'* consent.

The data owner may exercise the right of access free of any charge and the data owner may at any time request the withdrawal or blocking of his name from any of the databases referred to above.

Other rights

Every person has the right to rectify, update, and, when applicable, suppress or keep confidential his or her personal data included in a personal database. A number of specific rules apply to this process. In particular, if the personal data has been transferred to a third party, that third party must be notified of any rectification or suppression of personal data within five days of such amendments being made.

Security

Security requirements in order to protect personal data

The security obligations in the DPA are closely based on the *general data security obligations* but also include an express obligation to use measures to detect any unauthorised access or amendment to personal data.

There is also a duty of confidentiality that applies to any persons processing personal data. Such duty continues even after the relationship with the owner of the database has expired. The duty is only released by an order of the court or for reasons relating to public safety, national defence or public health.

There are also some specific security obligations set out in resolutions N° 11/2006 and N° 9/2008.

Specific rules governing processing by third party agents (processors)

In addition to the duty of confidentiality (see above), any third party providing data processing services may: (i) only use the relevant personal data for the purposes specified on the corresponding service contract; and (ii) not disclose that personal data to any third party, even for storage purposes.

Once the service contract has been performed, the relevant personal data must be destroyed, unless the owner of that data gives clear instructions to preserve the personal data, in which case it may be stored securely for a maximum of two years.

Notice of breach laws

None.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transfer of any type of personal information to countries or international or supranational entities which do not provide adequate levels of protection is prohibited.

The prohibition shall not apply to disclosures: (i) for the purpose of international judicial cooperation; (ii) for the purpose of healthcare or of anonymised personal data for the purpose of an epidemiological survey; (iii) for stock exchange or banking transfers; (iv) when subject to an international treaty to which the Argentine Republic is a signatory; (v) for international cooperation between intelligence agencies in the fight against organised crime, terrorism and drug trafficking; and (vi) where the data owner has expressly consented to the assignment.

Consent is not required for transfers of data from a register that is legally constituted to provide information to the public and which is open to consultation either by: (i) the public in general; or (ii) any person who can demonstrate legitimate interest, provided that in that particular case, the legal and regulatory conditions for the query are fulfilled.

Finally, an international data transfer agreement can be used to permit the transfer of personal data to a third country.

Notification and approval of national regulator (including notification of use of Model Contracts)

It is not necessary to notify or obtain approval from a national regulator for *transborder dataflow*.

Use of binding corporate rules

Argentina does not recognise the use of *binding corporate rules* as a means to justify *transborder dataflow*.

Enforcement

Sanctions

There are administrative and criminal penalties under the DPA.

Administrative sanctions can be applied by the Directorate and consist of a warning, suspension, closure of a database or a fine ranging between 250 USD and 25,000 USD.

There is a range of criminal penalties including: (i) imprisonment for up to two years for knowingly inserting false information in a personal database; (ii) imprisonment for up to three years for anyone who knowingly provides a third party with false information contained in a personal database; (iii) imprisonment for up to three years for hacking into a personal database; and (iv) imprisonment for up to three years for disclosing confidential information from a database. These penalties can be increased if harm is caused to a *data owner* or the offence is committed by a public official in the exercise of his duties.

Practice

Enforcement is relatively infrequent but there have been cases in which criminal complaints have been filed, for example against ChoicePoint for selling information about Argentinean citizens to the US government.

Moreover, some entities have received sanctions from the DPA for not renewing the databases at the proper time.

Enforcement authority

Administrative sanctions are issued by the Directorate. Criminal sanctions can only be imposed by the courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

There are no specific rules on ePrivacy matters.

Cookies

Conditions for use of cookies

None.

Regulatory guidance on the use of cookies

None.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Save as provided below there are no specific rules on direct marketing by e-mail. However, the sending of direct marketing by e-mail is subject to the general principles of the DPA.

Conditions for direct marketing by e-mail to corporate subscribers

Save as provided below there are no specific rules on direct marketing by e-mail. However, the sending of direct marketing by e-mail is subject to the general principles of the DPA.

Exemptions and other issues

When direct marketing e-mails are sent to someone, and the justification for sending that email is not consent, the e-mail must be prominently marked as advertising by including the word "publicidad" in the header.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Save as provided below there are no specific rules on direct marketing by telephone. However, direct marketing by telephone is subject to the general principles of the DPA.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Save as provided below there are no specific rules on direct marketing by telephone. However, direct marketing by telephone is subject to the general principles of the DPA.

Exemptions and other issues

In the jurisdiction of the City of Buenos Aires a "Do Not Call Registry" has been established to reduce excessive telemarketing calls. Any subscriber can join the “Do not call Registry” and thus avoid telemarketing calls.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

There are no specific rules on direct marketing by fax. However, the sending of direct marketing by fax is subject to the general principles of the DPA.

Conditions for direct marketing by fax to corporate subscribers

There are no specific rules on direct marketing by fax. However, the sending of direct marketing by fax is subject to the general principles of the DPA.

Exemptions and other issues

None.

Australia

Contributed by Allens

General | Data Protection Laws

National Legislation

General data protection laws

The Commonwealth of Australia has enacted the Privacy Act 1988 (the "**Privacy Act**"). It has also enacted other legislation granting privacy rights, including the Taxation Administration Act 1953, the Telecommunications Act 1997 and Telecommunications (Interception and Access) Act 1979.

Substantive amendments to the Privacy Act will come into effect on 12 March 2014. Significant changes to the current regulatory regime will be implemented in respect of a number of areas including direct marketing, privacy collection statements and privacy policies, collection of unsolicited personal information, disclosure of personal information outside Australia, credit reporting, pecuniary penalties and enforcement. It is expected there will be a further stage of privacy reforms in the future.

A number of Australian States and Territories have also enacted privacy legislation. In particular, New South Wales, the Northern Territory, Queensland, Tasmania and Victoria all have specific privacy laws. In addition, the Australian States and Territories have enacted a range of other legislation which provides privacy rights. This other legislation addresses issues such as surveillance, use of criminal record information and use of health information.

The remainder of this summary only considers the Privacy Act (except to the extent otherwise specified).

Entry into force

The Privacy Act came into effect on 1 January 1989. The Privacy Amendment (Private Sector) Act 2000 (Cth) came into effect on 21 December 2001, amending the Privacy Act to establish a national scheme to regulate private sector organisations' handling of personal data. The Privacy Amendment (Enhancing Privacy Protection) Act 2012 will come into effect on 12 March 2014 and will substantively amend the Privacy Act.

National Regulatory Authority

Details of the competent national regulatory authority

Office of the Australian Information Commissioner

GPO Box 5218
Sydney
NSW 2001

GPO Box 2999
Canberra
ACT 2601

www.oaic.gov.au

The Information Commissioner heads the Office of the Australian Information Commissioner and is supported by the Freedom of Information Commissioner and the Privacy Commissioner. In practice, the Privacy Commissioner is responsible for the majority of the privacy related functions of the Office of the Australian Information Commissioner, including the investigation of complaints made by *data subjects*.

The previous regulatory authority, the Office of the Privacy Commissioner, was integrated into the Office of the Australian Information Commissioner on 1 November 2010.

Notification or registration scheme and timing

There is no notification or registration scheme for organisations that handle personal data.

Exemptions

Not applicable.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The Privacy Act defines personal data (referred to in the Privacy Act as "personal information") differently to the *standard definition of personal data*. Under the Privacy Act, personal data means "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an

individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion". The distinction between these definitions is unlikely to be substantive.

Is information about legal entities personal data?

No, unless the legal entity is a *data subject*, for example a sole trader.

What are the rules for processing personal data?

The Privacy Act does not specifically refer to "processing" personal data and there is no distinction between entities which control, as opposed to process, personal data. This means that any handling of personal data, whether using, holding, processing or otherwise, is potentially subject to the Privacy Act. The Privacy Act contains a number of binding principles regarding the handling of personal data which apply to private sector organisations (National Privacy Principles or NPPs) and federal government agencies (Information Privacy Principles or IPPs).

While the NPPs contain obligations which are broadly similar in operation and effect to the *standard conditions for processing personal data*, these provisions are dispersed throughout the NPPs. The NPPs are grouped under the following subject matter headings: collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transborder data flows and sensitive information.

The NPPs provide, as a general rule, that an organisation should only use or disclose personal data for the purpose for which it was collected. However, an organisation may use or disclose personal data about a *data subject* for another purpose (a secondary purpose) if the *data subject* has consented or the secondary purpose is related to the primary purpose and such use or disclosure might reasonably be expected by the *data subject*. If the personal data is sensitive personal data, the secondary purpose must be directly related to the primary purpose. There are a number of exceptions to this general rule.

Are there any formalities to obtain consent to process personal data?

There are no specific formalities to obtain consent set out in the Privacy Act. Consent can be express or implied, written or oral, but in any event requires both knowledge of the matter agreed to and voluntary agreement of the relevant *data subject*. The level of consent required in any particular case will depend upon, among other things, the seriousness of the consequences for the *data subject* if the personal data were to be used or disclosed.

Sensitive Personal Data

What is sensitive personal data?

The Privacy Act defines sensitive personal data (referred to in the Privacy Act as "sensitive information") more broadly than the *standard types of sensitive personal data* by also including in the definition the following matters: (i) information or an opinion about a *data subject's* membership of a political or professional association or criminal record that is also personal data; and (ii) genetic information about a *data subject* that is not otherwise health information.

Are there additional rules for processing sensitive personal data?

Generally, an organisation is not allowed to collect sensitive information from a *data subject* unless the *data subject* has consented or the collection is required by law. An organisation can collect health information from a *data subject* without consent in certain limited circumstances. Non-profit organisations may collect sensitive information from a *data subject* without consent if the information relates solely to members or individuals who have regular contact with the organisation, and the organisation undertakes not to disclose the information without consent.

An organisation may only use or disclose sensitive data for a purpose other than the primary purpose of collection (secondary purpose) if the secondary purpose is directly related to the primary purpose of collection and such use or disclosure might reasonably be expected by the *data subject*, the *data subject* has consented or the use or disclosure is authorised or required under law.

Are there any formalities to obtain consent to process sensitive personal data?

There are no specific formalities to obtain consent set out in the Privacy Act. Consent can be express or implied, written or oral, but in any event requires both knowledge of the matter agreed to and voluntary agreement of the relevant *data subject*. The level of consent required in any particular case will depend upon, among other things, the seriousness of the consequences for the *data subject* if the personal data were to be used or disclosed.

Scope of Application

What is the territorial scope of application?

The Privacy Act applies to activities of organisations within Australia.

The Privacy Act also applies to the overseas activities of Australian organisations and foreign organisations which have a link with Australia. In each case, the Privacy Act applies to personal data of an Australian citizen or resident. The

exception to this is in the application of NPP 9, which relates to transfer outside Australia. NPP 9 applies to any personal data, irrespective of whether it relates to an Australian citizen or otherwise.

An organisation is considered to have a link with Australia if: (i) there is an organisational link: for example, the organisation is a company incorporated in Australia, or a trust created in Australia; or (ii) the organisation carries on business in Australia or an external Territory and the organisation collects or holds personal data in Australia or an external territory.

If an organisation's overseas activity is required by the law of a foreign country, then that activity is not taken to amount to an interference with the privacy of a *data subject*.

Who is subject to data protection legislation?

Private sector organisations and federal government agencies are subject to the Privacy Act. State and Territory government agencies are subject to separate State and Territory legislation.

The Privacy Act contains exemptions for certain organisations from the requirement to comply with the NPPs. For example, operators of small businesses (broadly, businesses with an annual turnover for the previous financial year of $3,000,000 or less) are not generally subject to the Privacy Act. There is an exemption for domestic use, media organisations and political parties. However, there is no general exemption for not-for-profit organisations.

There is a limited exemption from the application of the Privacy Act for the sharing of personal data (other than personal data that is sensitive data) between companies in the same group. Principles regarding the transfer of personal data outside Australia apply even where the transfer is between group companies.

There is no distinction between entities which control, as opposed to process, personal data. Any handling of personal information, whether holding, processing or otherwise, is potentially subject to data protection legislation.

Are both manual and electronic records subject to data protection legislation?

Yes. The Privacy Act applies to any personal data that is gathered, acquired or obtained from any source and by any means. The definition of personal data in the Privacy Act expressly includes reference to personal data forming part of a database.

Rights of Data Subjects

Compensation

Where a *data subject* has made a complaint in relation to the handling of personal data by an organisation, the Commissioner has the power to make a determination which includes declarations that: (i) the *data subject* is entitled to a specified amount to reimburse the *data subject* for expenses reasonably incurred in connection with the making and investigation of the complaint; and (ii) the *data subject* is entitled to a specified amount as compensation.

A determination of the Commissioner regarding an organisation is not binding or conclusive. However, the *data subject* or the Commissioner has the right to commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the determination.

Fair processing information

At the time of collection (or as soon as practicable afterwards) an organisation collecting personal data must take reasonable steps to make a *data subject* aware of the identity of the organisation and the purposes of the processing.

It must also provide information about: (i) the right of the *data subject* to access the personal data; (ii) the disclosure practices of the organisation; and (ii) any law that requires the particular personal data to be collected and the consequences (if any) for the *data subject* if the personal data is not provided.

Where personal data is not directly collected from the *data subject*, an organisation must take reasonable steps to make sure the *data subject* is informed of the same matters in respect of its indirect collection.

Rights to access information

As a general rule, an organisation must, upon request, give the *data subject* access to any personal data held about them. However, there are exceptions to this general rule including, by way of example, where the provision of access to personal data could have an unreasonable impact on the privacy of other *data subjects* or where denying access is required or authorised by or under law.

Objection to direct marketing

If an organisation wishes to rely on the direct marketing exemption to the obligations governing the use and disclosure of personal data, a *data subject* must be told that they can opt out of receiving any further marketing from that organisation. The direct marketing exemption only applies to the use of non-sensitive data for direct marketing where, among other things, it is impracticable to seek the *data subject's* consent.

Other rights

An organisation must take reasonable steps to correct any personal data if the *data subject* can establish that it is not accurate. If an organisation refuses to correct personal data, it must give reasons to the person who has requested such correction.

Wherever it is lawful and practicable, *data subjects* must have the option of not identifying themselves when entering transactions with the organisation.

A *data subject* may submit a complaint to the Commissioner about an act or practice that may be an interference with the privacy of the *data subject*. The complaint may then be investigated by the Commissioner.

Security

Security requirements in order to protect personal data

NPP 4 (entitled "Data Security") requires organisations to take reasonable steps to protect the personal data they hold from misuse, loss and unauthorised access, modification and disclosure. NPP 4 does not mandate any specific security obligations or standards. This differs from *general data security obligations* since it does not provide express guidance as to the matters that may be relevant or reasonable to consider in assessing compliance with this obligation.

Specific rules governing processing by third party agents (processors)

There are no specific rules governing the handling of personal data by third parties. The obligation placed on organisations under NPP 4 to take reasonable steps to protect personal data from misuse, loss and unauthorised access, modification and disclosure has the effect of requiring those organisations to take reasonable steps to ensure that any third party handling personal data on its behalf also takes the same steps to protect personal data.

Notice of breach laws

The Privacy Act does not contain any obligation to inform the Commissioner or *data subjects* of a security breach. However, the Commissioner has issued non-binding guidance stating that organisations should notify affected *data subjects* of a breach where there is a real risk of serious harm as a result of the breach.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transborder data flow restrictions set out at NPP 9 in the Privacy Act differ substantively from the *standard conditions for transborder dataflow*.

NPP 9 provides that an organisation may transfer personal data to someone who is outside Australia only if: (i) the organisation reasonably believes that the recipient is subject to a law, binding scheme or contract which is substantially similar in effect to the NPPs; (ii) the *data subject* consents to the transfer of the personal data; or (iii) the organisation has taken reasonable steps to ensure that the personal data which it has transferred will be held, used or disclosed by the recipient in a manner consistent with the NPPs; (iv) the transfer is necessary for the performance of a contract between the *data subject* and the organisation, or for the implementation of pre-contractual measures taken in response to the *data subject's* request; (v) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the *data subject* between the organisation and a third party; or (vi) all of the following apply: (i) the transfer is for the benefit of the *data subject*; (ii) it is impracticable to obtain the consent of the *data subject* to that transfer; and (iii) if it were practicable to obtain such consent, the *data subject* would be likely to give it.

The obligation placed on organisations under NPP 4 to take reasonable steps to protect personal data from misuse, loss and unauthorised access, modification and disclosure will apply to the transfer of personal data to an overseas recipient. Organisations transferring personal data to overseas recipients will need to ensure that the personal data will continue to be secure once transferred. Once an organisation transfers personal data to an organisation in a foreign country, the Privacy Act will apply to the overseas organisation only to the extent set out in the section entitled “What is the territorial scope of application?”.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no ability for organisations to transfer personal data overseas subject to the prior notification and approval of the Commissioner.

Use of binding corporate rules

There is currently no ability for organisations to use *binding corporate rules* in respect of the cross-border transfer of personal data.

Enforcement

Sanctions

The Commissioner has the option to respond to complaints made by *data subjects*, launch the Commissioner's own investigation of privacy breaches (referred to as "own-motion investigations") or seek injunctive relief in respect of contraventions of the Privacy Act.

In response to complaints made by *data subjects*, the Commissioner has the power, among other things, to attempt, by conciliation, to effect a settlement of the matters that gave rise to the investigation or to make a determination which includes declarations that: (i) the *data subject* is entitled to a specified amount to reimburse the *data subject* for expenses reasonably incurred in connection with the making and investigation of the complaint; (ii) the *data subject* is entitled to a specified amount as compensation; (iii) the organisation has engaged in conduct constituting an interference with the privacy of a *data subject* and that it must not repeat or continue such conduct; and (iv) the organisation perform any reasonable act or course of conduct to redress any loss or damage suffered by the *data subject*.

While a determination of the Commissioner made as a result of an investigation following a complaint is not binding or conclusive, the respondent organisation must not repeat or continue the conduct covered by the declaration and must perform the act or course of conduct covered by the declaration. However, this obligation does not extend to a declaration regarding the payment of compensation. The *data subject* or the Commissioner has the right to commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the determination. If this occurs, the court will consider the question as to whether or not the respondent organisation breached the Privacy Act by way of a hearing de novo.

The Commissioner's powers in response to own motion investigations are currently extremely limited. The Commissioner does not have the power to make determinations or declarations in respect of an own motion investigation. Action taken by the Commissioner following an own motion investigation has included the provision of advice and the facilitation of apologies, appropriate disposal of records and changes to the privacy related practices and procedures of organisations.

Practice

According to the Office of the Australian Information Commissioner's 2011-12 Annual Report, the Office received 1,357 complaints, 2822 written enquiries and 21,317 telephone enquiries in the year ending 30 June 2012.

The Commissioner made one determination in 2011–12, in which the Commissioner declared that the respondent apologise in writing to the complainant, review its staff training regarding the handling of personal information, advise the Commissioner of the outcome of the training review, and pay the complainant $7500.

The Commissioner undertook 37 investigations on its own motion and received 46 notifications of data breaches from organisations during the same period.

In the majority of cases, organisations the subject of a complaint or own motion investigation undertook action to resolve issues either on their own initiative or in accordance with the recommendations of the Commissioner.

Enforcement authority

While a determination of the Commissioner made as a result of an investigation following a complaint is not binding or conclusive, the respondent organisation must not repeat or continue the conduct covered by the declaration and must perform the act or course of conduct covered by the declaration. However, this obligation does not extend to a declaration regarding the payment of compensation.

The *data subject* or the Commissioner has the right to commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the determination. If this occurs, the court will consider the question as to whether or not the respondent organisation breached the Privacy Act by way of a hearing de novo.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Spam Act 2003 (Cth) (the "**Spam Act**") governs the sending of commercial electronic messages. Its key operative provisions came into force on 10 April 2004.

The Do Not Call Register Act 2006 (Cth) (the "**DNCR Act**") and Do Not Call Register Regulations 2006 govern telemarketing and fax marketing. The operative sections of the DNCR Act took effect on 31 May 2007. The Telemarketing and Research Industry Standard 2007 and the Fax Marketing Industry Standard 2011 have also been implemented (from 31 May 2007 and 4 May 2011 respectively) and regulate telemarketing and fax marketing in addition to the DNCR Act.

Both the Spam Act and the DNCR Act are regulated by the Australian Communications and Media Authority (www.acma.gov.au).

Cookies

Conditions for use of cookies

The use of cookies is not specifically regulated in Australia. However, personal data collected via the use of cookies is subject to Australian privacy laws in the same manner as all other personal data.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The Spam Act requires that all "commercial electronic messages" identify the sender and, unless exempt, be sent with the consent of the recipient and include a functional unsubscribe mechanism.

The Spam Act regulates the sending of commercial electronic messages which have an "Australian link", which is where: (i) the sending of the message was authorised by a *data subject* physically present in Australia when the message was sent; (ii) the organisation who sent the message is an organisation whose central management and control is in Australia when the message is sent; or (iii) the relevant electronic account-holder is a person who is physically present in Australia at the time the message is accessed or is an organisation that carries on business or activities in Australia at the time the message is accessed.

Conditions for direct marketing by e-mail to corporate subscribers

The Spam Act does not distinguish between individual and corporate recipients of commercial electronic messages.

Exemptions and other issues

Exemptions from the Spam Act requirements include certain messages authorised by government bodies, registered political parties, religious organisations and charities or charitable institutions, subject to certain conditions.

Commercial electronic messages may be sent where consent is obtained. Consent may be express or inferred from the conduct of the person and the business or other relationship between the sender and the person. In limited circumstances, consent may be inferred from publication of an email address.

Civil penalties are among the remedies that may apply where an organisation has breached the Spam Act.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The DNCR Act establishes a compulsory Do Not Call Register (the "**Register**") of telephone numbers belonging to individuals who have opted out of receiving telemarketing calls. Individuals are able to submit their Australian fixed line or mobile domestic telephone numbers to be recorded on the Register. With some exceptions, it is an offence to make an unsolicited telemarketing call to any registered number. For the purposes of the DNCR Act, "telemarketing call" is defined as a voice call (including recorded or synthetic voices) to a telephone number with a commercial purpose.

The DNCR Act allows organisations seeking to make or authorise telemarketing calls to submit a list of Australian telephone numbers to the ACMA for checking against the Register so as to identify and eliminate from that list the telephone numbers of those people who have listed their telephone number on the Register – a practice known as "washing". A "washed" list may for a certain time be relied upon by the person submitting it as stating a list of telephone numbers to which telemarketing calls may be made without breaching the DNCR Act.

Telemarketing activities applying to numbers not entered on the Register or conducted by organisations not subject to the DNCR Act are governed by the Telemarketing and Research Industry Standard 2007 (the "**TRCI Standard**"). The TRCI Standard establishes minimum standards in relation to the hours and days that telemarketing and research calls are able to be made, the nature, purpose and source of telemarketing or research calls, the termination of telemarketing calls upon the request of the recipient and the provision of calling line information.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

An Australian number is eligible to be entered on the Register if it is: (i) used or maintained primarily for private or domestic purposes; (ii) used or maintained exclusively for transmitting and/or receiving faxes; (iii) used or maintained exclusively for use by a government body; or (iv) an emergency service number.

Telemarketing calls to corporate subscribers, unless they fall into one of the categories above, are therefore unlikely to be caught by the DNCR Act. Telemarketing activities applying to numbers not entered on the Register or conducted by organisations not subject to the DNCR Act are governed by the TRCI Standard.

Exemptions and other issues

Exemptions from the DNCR Act requirements include calls authorised by government bodies, religious organisations and charities or charitable institutions, subject to certain conditions. However, such entities may be covered by the TRCI Standard when making specific types of telemarketing calls.

Telemarketing calls may be made to a telephone number which is registered on the Register if the relevant person has consented to receiving such calls. Consent may be express or inferred from the conduct of the person and the business or other relationship between the marketer and the person.

Remedies for breach of the DNCR Act include civil penalties and injunctions.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The conditions for fax marketing under the DNCR Act are similar to those for telemarketing.

Fax marketing activities applying to numbers not entered on the Register or conducted by organisations not subject to the DNCR Act are governed by the Fax Marketing Industry Standard 2011 (the "**FMI Standard**"). The FMI Standard establishes minimum standards in relation to the hours and days that marketing faxes are able to be sent, the types of information required to be included on marketing faxes, the provision of opt-out information and limitations on the quantities of marketing faxes able to be sent to a recipient.

Conditions for direct marketing by fax to corporate subscribers

An Australian number is eligible to be entered on the Register if it is: (i) used or maintained primarily for private or domestic purposes; (ii) used or maintained exclusively for transmitting and/or receiving faxes; (iii) used or maintained exclusively for use by a government body; or (iv) an emergency service number.

Fax marketing activities applying to numbers not entered on the Register or conducted by organisations not subject to the DNCR Act are governed by FMI Standard.

Exemptions and other issues

Exemptions from the DNCR Act requirements include marketing faxes authorised by government bodies, religious organisations and charities or charitable institutions, subject to certain conditions. However, such entities may be covered by the FMI Standard when making specific types of marketing faxes.

Fax marketing activities may be made to a telephone number which is registered on the Register if the relevant person has consented to receive the marketing fax. Consent may be express or inferred from the conduct of the person and the business or other relationship between the marketer and the person.

Remedies for breach of the DNCR Act include civil penalties and injunctions.

Austria

Contributed by Schönherr Rechtsanwälte GmbH

General I Data Protection Laws

National Legislation

General data protection laws

The Federal Act concerning the Protection of Personal Data (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000)) (the "**DPA**"), dated 17 August 1999, implemented the *Data Protection Directive* in Austria. The DPA was last substantially revised on 1 January 2010 where, inter alia, specific CCTV provisions and a "data breach notification duty" were introduced. Currently there is another revision of the DPA pending. The revised DPA will allow companies to establish a data protection officer on a voluntarily basis. The revised DPA will not force companies to appoint a data protection officer but if a company decides to do so it will no longer be obliged to notify its data processing activities to the Data Protection Commission. The revised DPA is expected to enter into force during the first half of 2013.

Entry into force

The DPA came into force on 1 January 2000.

National Regulatory Authority

Details of the competent national regulatory authority

Austrian Data Protection Commission (the "**Data Protection Commission**")
Hohenstaufengasse 3
1010 Vienna
Austria

www.dsk.gv.at

Notification or registration scheme and timing

Unless the respective data processing is exempt (see below), the *data controller* has a general obligation to file a notification with the Data Protection Commission. Such notification is registered at the Data Processing Register which is an organisational unit of the Data Protection Commission. Registration fees are currently an overall fee of EUR 13.20 and another fee of EUR 6.50 per application. The notification must be made prior to the commencement of data processing. However, if the data to be processed: (i) are not sensitive personal data; (ii) are not related to criminal content; (iii) do not include any information about the credit ranking of the *data subject*; (iv) will not be processed within a joint information system (*Informationsverbund*); and (v) are not taped in the course of CCTV monitoring, the data processing can be launched before the registration is completed. Notification proceedings frequently take several months, sometimes even up to a year to complete.

In 2012 the registration procedure substantially changed. Registration now has to be done via the "DVR Online" System, which can be accessed via the webpage of the Data Protection Commission. The "DVR Online" System follows a self registration approach whereby the company registers its data processing activities through this system. The Data Protection Commission then assesses the conclusiveness and legitimacy of the proposed registration and will follow up with questions to the company if it feels there is a need for further clarifications.

Exemptions

Exemptions apply in specific circumstances, including but not limited to: (i) processing of published data; (ii) processing of personal data not linked to a name; or (iii) "standardised" data processing. The latter exemption refers to specific data applications of standardised character defined by an ordinance (for example, accounting or specific CCTV scenarios). If the actual data to be processed equates to one of those standardised data applications, the data processing will be exempt from notification.

Appointment of a data protection officer

Currently, there is no legal requirement to appoint a data protection officer. However, as noted above, there are plans under a revised DPA for the introduction of an option to appoint a data protection officer on a voluntary basis.

Personal Data

What is personal data?

The DPA defines personal data as any information relating to any person or group of persons being different from the *data controller*. In its settled case law, the Data Protection Commission frequently interprets this definition in the broadest

sense, considering all kinds of information as personal data whenever such information can be linked to an individual or legal entity (see below).

Is information about legal entities personal data?

Yes. Contrary to the *standard definition of personal data* the definition of personal data under the DPA extends to data relating to both individuals and legal entities. Austria is one of the few countries to extend local data protection law to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, both consent and the legitimate interests condition are frequently relied upon as grounds for the processing of non-sensitive data. The legitimate interests condition is more highly favoured as the Austrian judicature has set out very strict requirements for obtaining a *data subject's* consent (see below).

The DPA contains exemptions for certain types of data processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA. There are also specific provisions in place for the processing of data for scientific research purposes. Moreover, processing of indirect personal data is only partially subject to the provisions of the DPA. Indirect personal data is any kind of data relating to an individual where the *data controller* has no possibility of revealing the identity of the *data subject* (for example, encrypted data that cannot be decrypted by the *data controller*).

Are there any formalities to obtain consent to process personal data?

In principle, consent can be given in writing, orally or even implied. However, as previously stated, the Austrian judicature set out very strict requirements for a *data subject's* consent to be valid: (i) the *data subject* must be provided with all relevant information about the data to be processed, the purpose of the respective data processing and any potential data recipients; (ii) the consent must be given without any restraints (hence, the Austrian courts are frequently reluctant to accept the validity of employee consent); and (iii) the *data subject* has to receive explicit information about his right to revoke his consent at anytime, without giving reason for such revocation.

Sensitive Personal Data

What is sensitive personal data?

The definition of sensitive data under the DPA equates to the *standard types of sensitive personal data*.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. However, the DPA provides some additional legal grounds for processing of sensitive data such as, but not limited to, use for domestic or scientific research purposes. While processing of non-sensitive data only requires notification, any processing of sensitive data requires the (additional) approval of the Data Protection Commission. Although not explicitly listed as sensitive data under the DPA, any processing of criminal-related data also requires approval of the Data Protection Commission.

Are there any formalities to obtain consent to process sensitive personal data?

In principle, the position is the same as for the processing of personal data (see above) with the exception that consent has to be given expressly, which means that implied consent will not be sufficient.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The DPA applies to *data controllers*. Several provisions of the DPA also apply to *data processors*.

Are both manual and electronic records subject to data protection legislation?

Yes, the DPA applies to electronic and manual records, provided the manual records are structured in a way that they can be searched via a search key (for example, a cardbox). However, in practice manual records are of secondary importance as nearly all decisions of the Data Protection Commission and Austrian Courts involve electronic records and electronically processed data.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation if they suffer damage from unlawful data processing. If personal data which has been processed in breach of the DPA is published, the affected *data subject* also has a right to compensation for

distress. However, only few cases have been brought to court so far where *data subjects* have sought compensation for breaches of the DPA.

Fair processing information

A *data controller* must provide *fair processing information* to *data subjects*. Additionally, he must provide the *data subject*, upon request, with a list of the processed data and a description of the origin of the data, the legal basis for the data processing and the recipients of the data (if any). Such information is mandatory and has to be given within eight weeks; if the *data controller* fails to provide adequate information, the *data subject* will be entitled to file a complaint with the Data Protection Commission. The *fair processing information* does not necessarily have to refer to the DPA but should be provided in German in order to ensure it is fairly provided.

Rights to access information

Upon request, the *data controller* has to provide *subject access information* to the *data subject* within eight weeks (compare above: he may also provide copies of that data). In practice such requests are virtually always made and answered in writing. Initially, such subject access requests are free of charge. However, if the *data subject* has already made an identical subject access request within the same year, the *data controller* would be entitled to charge a flat rate fee of EUR 18.89 for the second (or any subsequent) request. The *data controller* may raise this flat rate compensation charge in order to cover actually incurred higher expenses. Under the DPA the right to access information only applies to the *data controller*. If a *data processor* receives such a request for information it must be forwarded to the *data controller* he is acting for.

Objection to direct marketing

Art 14b of the Directive has not been implemented in the DPA due to the fact that Section 151 of the Austrian Trade Act (Gewerbeordnung 1994) provides for all data of a *data subject* being processed for the purposes of direct marketing to be erased within eight weeks upon request of the *data subject*. In addition, Section 151 of the Austrian Trade Act provides for the possibility of a person registering at the Austrian Chamber of Commerce which prevents the registered person from receiving postal marketing and advertising. A similar register with respect to marketing by e-mail is administered by the Austrian Regulator for Broadcasting and Telecommunications (the "RTR").

Other rights

The *data subject* can apply for rectification and erasure of data that are incorrect, outdated or that have been processed in breach of the DPA.

The *data subject* has the right to raise an objection to the processing of its personal data if the processing is not authorised by law and the use of data infringes an overriding interest of secrecy deserving protection that arises from the particular situation. If the respective data is stored in a publicly available database the *data subject* is entitled to raise an objection without giving further reason. In this connection, the Austrian Supreme Court ruled that a *data subject* is entitled to object, without reason, to the processing of his personal data without giving reason when such data is processed within a credit report database (Bonitätsdatenbank).

Security

Security requirements in order to protect personal data

The security obligations of the DPA go beyond the *general data security obligations*. There are several specific security requirements to be met, such as (but not limited to): (i) the use of data must be tied to valid instructions of the authorised organisational units or users; (ii) every user is to be instructed about his duties according to the DPA and the organisation's internal data protection regulations, including data security regulations; (iii) the right of access to the premises of the *data controller* or *data processor* is to be regulated; (iv) the right of access to data and programs is to be regulated as well as the protection of storage media against access and use by unauthorised persons; (v) every device is to be secured against unauthorised operation by ensuring that security processes are in place in both the machines and programs used; and (vi) logs of the processing steps must be kept.

Specific rules governing processing by third party agents (processors)

There are several specific rules that apply to data processing performed by a *data processor* on behalf of a *data controller*. The *data processor* must: (i) use data only according to the instructions of the *data controller*; (ii) take all required safety measures pursuant to Section 14 of the DPA (in particular, employ only users who have committed themselves to confidentiality vis-à-vis the *data processor* or are under a statutory obligation of confidentiality); (iii) enlist another *data processor* only with the permission of the *data controller*; (iv) insofar as possible given the nature of the processing, create in agreement with the *data controller* the necessary technical and organisational requirements for the fulfilment of the *data controller's* obligation to grant the right of information, rectification and erasure; (v) hand over to the *data controller* the results of processing and documentation containing data or keep or destroy them at the *data controller's* request after the processing of data is finished; and (vi) make available to the *data controller* all information necessary to control compliance with these obligations.

Notice of breach laws

On 1 January 2010 a "data breach notification duty" was introduced to the DPA. *Data controllers* are obliged to inform *data subjects* if they become aware of systematic and seriously unlawful misuse of the *data subjects'* data. However, this duty for information does not take effect if the data misconduct only has the potential to cause minor harm to the affected *data subjects* or if the costs of proper information would be disproportionally high. Note that the DPA does not require any authority be notified of the breach. In particular, the DPA does not ask for the Data Protection Commission to be informed.

In October 2011 the Austrian Telecommunications Act was revised in order to comply with the *Citizens' Rights Directive*. Inter alia, this revision brought a duty for communications providers to inform the Data Protection Commission in case personal data has been breached.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transfer of personal data to countries outside the EU is subject to approval of the Data Protection Commission, based upon the following conditions: (i) legitimacy of the data application being filed; (ii) proof of an adequate level of data protection of the receiving party; and (iii) proper protection of secrecy interests. Approval of the Data Protection Commission will not be needed if the data transfer is based on specific, valid legal grounds such as, but not limited to, the *data subject's* consent or if the personal data are transferred to countries which guarantee an adequate level of protection or if the data are transferred to safe harbor companies. However, notification and registration will still be required.

Notification and approval of national regulator (including notification of use of Model Contracts)

As mentioned above, notification and approval of the Data Protection Commission will be required if personal data is to be transferred to countries outside the EU (for approval exemptions, see above). If the data transfer is based on appropriate *Model Contracts* as set out by the EU, approval of the Data Protection Commission will still be required but, in practice, the respective approval proceedings are easier to accomplish. However, approval proceedings may easily take several months, sometimes even up to a year.

Use of binding corporate rules

The Austrian Data Protection Commission has approved the use of *binding corporate rules*. However, applications for approval of international data transfers are rarely based upon *binding corporate rules* as applicants frequently rely on *Model Contracts* instead.

Enforcement

Sanctions

Breaches may incur civil, criminal and administrative sanctions, depending on the type of breach. The maximum penalty for deliberate violation of the provisions of the DPA dealing with data secrecy is EUR 25,000 and EUR 10,000 for violation of the notification and information obligations. Note that no administrative penalty may be imposed if the violation is subject to criminal prosecution.

Practice

According to the 2011/12 Data Protection Commission report, from 2010 to 2011 the Data Protection Commission dealt with 203 complaints from *data subjects*, with 565 "ombudsman" complaints (where the Data Protection Commission is not entitled to release binding decisions but rather recommendations) and 90 approvals of international data transfers. The Data Processing Register dealt with 19,435 applications for registration.

There is no statistical data on criminal prosecutions for data abuse available, as Section 51 of the DPA, which provides for a criminal penalty of up to one year's imprisonment, is only a subsidiary provision and therefore applies only if no other sanctions of more severe character pursuant to other provisions of the Criminal Code apply. Therefore, prosecution for data abuse will typically be subsumed within prosecution for other crimes (fraud, "cyber crimes" and, for the public sector, abuse of authority).

While the Data Protection Commission is competent for assessing whether a breach of the DPA took place, administrative fines for such breaches of the DPA are imposed by local administrative authorities (which frequently rely on the findings of the Data Protection Commission). Due to the multiplicity of these authorities there is no statistical data available on the level of penalties.

Enforcement authority

The Data Protection Commission is authorised to examine data applications and to order the *data controller* or *data processor* of the examined data application to grant access to the data applications and relevant documents. In the course of such examination proceedings the Data Protection Commission has certain competencies such as, but not limited to,

the right to: (i) enter premises where data applications are carried out; (ii) operate data processing equipment; or (iii) run the processing to be examined.

In addition, the Data Protection Commission may, inter alia, file lawsuits before the competent court of law or criminal charges with the Public Prosecutor. However, as mentioned above, administrative fines will be imposed by local administrative authorities but not by the Data Protection Commission.

The 2010 revisions to the DPA will increase the enforcement powers of the Data Protection Commission. These changes will become effective in 2012.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Section 107 of the Telecommunications Act (Telekommunikationsgesetz 2003) (the "TKG") implemented Article 13 of the *Privacy and Electronic Communications Directive*. Section 107 of the TKG came into force on 20 August 2003 and was last revised on 1 March 2006.

The TKG revision in October 2011 also included amendments in order to comply with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Despite having been revised, currently the TKG does not expressly address the conditions for use of cookies nor does it expressly clarify whether the use of browser settings can be qualified as consent for the use of cookies. Instead, it refers to an obligation of telecommunications or e-commerce service providers to provide the user with all embracing information about the collecting and processing of his personal data. The TKG also makes clear that the user's data must only be collected if he has given his consent. This does not, however, introduce a new concept, but rather confirms the existing legal status. Given this current legal framework, most of the Austrian legal professionals take the view that the required consent can be declared through browser settings, provided the user received appropriate information in advance. However, there is currently no statute or case law confirming this position.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

It is only permissible to send unsolicited direct marketing e-mails if the recipient has given his prior consent.

Conditions for direct marketing by e-mail to corporate subscribers

As this opt-in principle applies to corporate relations as well, it is only permissible to send unsolicited direct marketing e-mails to a corporate subscriber if he has given his prior consent.

Exemptions and other issues

Within already existing customer relationships it is permitted to send e-mails to customers for the purpose of direct marketing if the *similar products and services exemption* applies. In this respect it is important to note that the recipient can object to direct marketing e-mails through registration in a public opt-out list, which has been established pursuant to Section 7 of the E-Commerce Act and which is administered by the RTR. As subscribers are entitled to revoke their consent anytime, Section 107 of the TKG also prohibits direct marketing e-mails if the identity of the sender is disguised or concealed or if an opt-out address is not provided in the e-mails. The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make direct calls for marketing purposes to individual subscribers without their prior consent. It is also not permitted to make calls in order to obtain the subscriber's approval for subsequent direct marketing calls.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

As this opt-in principle applies to corporate relations as well, it is also not permissible to make direct calls for marketing purposes to corporate subscribers without their prior consent. Again, it is also not permissible to make calls in order to obtain the subscriber's approval for subsequent direct marketing calls.

Exemptions and other issues

Consent of corporate subscribers might be assumed if their contact address, phone and fax number is published on their website. However, there has been no clarifying judicature on this matter so far. Additionally, Section 151 of the Austrian Trade Act authorises address and marketing undertakings, within certain limits, to contact subscribers for their business purposes.

Subscribers can revoke their consent anytime. In order to facilitate subscriber revocation of their consent, callers must provide the subscribers with information about the caller's identities and their contact details.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to perform direct marketing by fax to individual subscribers without their prior consent. It is also not permissible to make calls in order to obtain the subscriber's approval for subsequent direct marketing by fax.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to perform direct marketing by fax to corporate subscribers without their prior consent. Again, it is also not permitted to make calls in order to get the subscriber's approval for subsequent direct marketing by fax.

Exemptions and other issues

Consent of corporate subscribers might be assumed if their contact address, phone and fax number are published on their website. However, there has been no clarifying judicature on this matter so far. Additionally, Section 151 of the Austrian Trade Act authorises address and marketing undertakings, within certain limits, to contact subscribers for their business purposes. Subscribers can revoke their consent at any time. In order to facilitate subscriber revocation of their consent, callers must provide the subscribers with information about the callers' identities and their contact details.

Belgium.

General I Data Protection Laws

National Legislation

General data protection laws

The law of 8 December 1992 on privacy protection in relation to the processing of personal data (the "**DPA**") was modified by the law of 11 December 1998 to implement the *Data Protection Directive*. Some provisions of the DPA have been modified, mainly by the law of 22 August 2002 on patients' rights and by the law of 26 February 2003 regarding the status and competence of the national regulatory authority.

Entry into force

The DPA entered into force on 1 September 2001 further to an implementing Royal Decree of 13 February 2001 (the "**Decree**").

National Regulatory Authority

Details of the competent national regulatory authority

Commission for the Protection of Privacy (the "**Commission**")
Rue de la Presse 35
1000 Brussels
Belgium

www.privacycommission.be

Notification or registration scheme and timing

The *data controller* must notify the Commission before the start of any wholly or partially automated processing operation. Such notification is a mere filing of information that can be made by electronic means, including any change thereto. It costs EUR 25 online or EUR 125 if made by hard copy. The end of any processing must also be notified.

Exemptions

Notification is only required for automated processing (and not for manual files) with certain exemptions applicable under strict conditions (e.g. payroll and personnel administration, accounting and client/supplier administration).

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA closely follows the *standard definition of personal data*.

However, Belgium has widened its interpretation of the concept of personal data by limiting the circumstances in which personal data can be considered anonymised. Indeed, as soon as a *data subject* can directly or indirectly be identified on the basis of a set of data, this data will be considered as personal data. This is true even if the person with the means to identify the individual behind the data is not the *data controller*.

Is information about legal entities personal data?

No. The concept of personal data only applies to individuals (including sole traders) as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. Furthermore, Belgian law specifies that the processing must be carried out with the unambiguous consent of the *data subject*.

In practice, the legitimate interest condition is frequently relied upon as a ground for processing non-sensitive personal data. However, the Commission insists that obtaining consent is best practice and the legitimate interest condition is a residual ground for processing that can only be used in circumstances where all other principles of the DPA continue to be complied with.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

Except with respect to the processing of sensitive personal data (see below), the DPA does not impose any formalities to obtain consent to process personal data. Such consent may be express or implied, written or oral. However, express and

written consent is recommended, for evidential purposes, as the DPA requires consent to be unambiguous. In addition, the DPA requires that consent be freely given, specific and informed.

As regards the processing of employees' personal data, the Commission recommends that such processing should be based on legal grounds other than consent since obtaining valid consent from employees may be difficult given their subordinate link to their employer. To the extent that such processing would still be consent based, the Commission recommends that one should obtain both individual consent, from the employee, and collective consent, through employee representative bodies such as the works council.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data is defined by reference to the *standard types of sensitive personal data*. In addition, data of a judicial nature such as information about criminal offences or criminal proceedings (including suspicions of such) is treated as sensitive personal data.

Are there additional rules for processing sensitive personal data?

Standard types of sensitive personal data may only be processed if the *standard conditions for processing sensitive personal data* are met. Please also note that consent is not a justification for processing personal data of a judicial nature.

In addition, for the processing of sensitive personal data the *data controller* must ensure that the persons having access to such data will comply with the obligation of confidentiality in relation to such data by means of legal or contractual provisions. The *data controller* must keep a list at the disposal of the Commission with the categories of persons having access to such data and a precise description of their roles in relation to the data.

Are there any formalities to obtain consent to process sensitive personal data?

Consent from a *data subject* to process *standard types of sensitive personal data* must be in writing.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The DPA primarily applies to *data controllers*, with limited obligations imposed on *data processors*.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to the processing of personal data carried out, in whole or in part, by automatic means as well as the processing of personal data other than by automatic means which forms part of a filing system (i.e. any structured set of personal data that are accessible according to specific criteria, whether centralised, decentralised or allocated on a functional or geographical basis).

Rights of Data Subjects

Compensation

Data subjects have a right to compensation by the *data controller* if they suffer damage. Such right is based on general Belgian liability law.

Fair processing information

A *data controller* must provide *fair processing information* to *data subjects*, including the recipients or categories of recipients of the data. In practice, such information is preferably provided in writing to the *data subjects* but this is not mandatory.

There is no obligation in the DPA to provide this information in any of the national languages of Belgium; however, it may be difficult to show that the information has been fairly provided if it is not in a language the *data subject* is familiar with. In addition, specific rules regarding the use of languages in Belgium should be taken into account, including those applicable in the context of an employment relationship.

Rights to access information

Upon request, the *data controller* must provide the *subject access information* to the *data subject*, free of charge.

Objection to direct marketing

If the data are to be used for direct marketing purposes, the *data subject* also has the right to object, free of charge, to such processing and the *data controller* must inform the *data subjects* of their right to object. To exercise such right, the

data subject must send a dated and signed request to the *data controller*, who must confirm the amendment or deletion within one month to the *data subject* and, where possible, the third parties to whom the incorrect data was communicated.

Other rights

The *data subject* has the right to have inaccurate data corrected or deleted.

In certain cases, the *data subject* may object to decisions being made about him/her based solely on automatic processing.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations* and must also: (i) secure access to the data; (ii) inform its personnel about their obligations under the DPA; and (iii) ascertain that no unlawful use is made of the software programs used for the automatic processing of personal data.

Specific rules governing processing by third party agents (processors)

The DPA requires that if the processing is carried out by a *data processor*, the *data controller* must conclude an agreement with the *data processor* containing the *standard processor obligations* as well as the allocation of liability between the *data processor* and the *data controller*. The obligations of this agreement must be provided for in writing or in an electronic format.

Notice of breach laws

The DPA does not contain any obligation to inform the Commission or *data subjects* of a security breach. However, *data controllers* in certain sectors may be required to inform sector regulators of particular types of breach.

A specific notice of breach obligation now applies to the electronic communications sector as a result of the implementation into national law of the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the *data controller* satisfies the *standard conditions for transborder dataflow*. Furthermore, the DPA states that permission for transfer to countries that do not guarantee an adequate level of protection may be granted by Royal Decree subject to adequate safeguards, including contractual guarantees.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no obligation to notify or obtain the consent of the Commission to any *transborder dataflows*; in particular, there is no obligation to notify or obtain its consent to the use of the *Model Contracts*.

However, such dataflows, including the use of the *Model Contracts* as justification, must be included in the notification of the processing to the Commission. Recently, the Commission has also requested that the *data controller* provide a copy of the Model Contract in such a notification if it is to be used to validate a transfer.

Use of binding corporate rules

The Commission has approved the use of *binding corporate rules* in Belgium. Such *binding corporate rules* must be ratified by an individual Royal Decree (issued by the Ministry of Justice after advice from the Commission).

Enforcement

Sanctions

The DPA provides for criminal sanctions for most provisions, including the duty to inform the *data subject* and the duty to file a prior notification. Penalties range from EUR 550 to EUR 550,000 and include, in specific cases, imprisonment of up to two years. The publication of the judgment may also be ordered, together with other measures that may constitute a serious threat to the *data controller*, such as confiscation of the support media, an order to erase the data, and/or a prohibition on using the personal data for up to two years.

Practice

In 2011, 2,866 new files were opened, 2,413 files closed during the same year of which 90% were finalised within 3 months (compared to 2,832 files opened and 2,220 closed in 2010).

The Commission has changed its system of registration of investigation files, therefore it is not possible to compare the detailed figures of 2011 with those of 2010. However, the types of files which were most commonly handled by the Commission in 2011 relate to: (i) processing of images (e.g. CCTV, right of image, YouTube): 572 files; (ii) general data protection principles (e.g. right of access and correction, transparency, etc.): 458 files; (iii) public authorities and privacy: 286 files; and (iv) trade practices (e.g. direct marketing, phishing, spam, data trading, etc.): 290 files.

In relation to the number of prosecutions last year, no information about individual complaints is available once the files are closed by the Commission.

Enforcement authority

The Commission's mission is, amongst other things, to monitor overall compliance with the DPA. To this end, the Commission has general power of investigation with respect to any type of processing of personal data as well as filing a criminal complaint with the Public Prosecutor. The Commission may also institute a civil action before the President of the Court of First Instance. However, the Commission cannot impose fines upon individuals or organisations.

An example is the current Yahoo! case regarding its refusal to hand over IP addresses to the public prosecutor. This ongoing case has already led to two Supreme Court judgments and is currently pending before the Antwerp Court of Appeal.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Belgian ePrivacy laws are contained in: (i) Articles 13 and 14 of the law of 11 March 2003 on certain legal aspects of information society services (the "**ECA**") and the Royal Decree of 4 April 2003 on the sending of advertising by e-mail (the "**RD**"), with regard to e-mails; and (ii) Article 100 of the Act on Market Practices and Consumer Protection of 6 April 2010 (the "**MPCP**"), all of which implemented Article 13 of the *Privacy and Electronic Communications Directive*.

Belgian law has been amended to implement some, but not all, the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

The cookie requirements in the *Citizens' Rights Directive* has been implemented into Belgian law. It is only possible to use cookies if: (i) clear and specific information has been provided to the individual regarding the purposes of the data processing and their rights, all in accordance with the general requirements of the DPA; and (ii) the individual provides consent after receiving this information. These restrictions do not apply to cookies that are strictly necessary for a service requested by an individual. The user must be allowed to withdraw their consent free of charge.

Compliance with these requirements is in addition to the general data protection obligations under the DPA.

Regulatory guidance on the use of cookies

As in most other Member States, the law does not specify how consent from users should be obtained. This matter will have to be clarified through regulatory guidance. The Commission reviewing the draft bill opined that consent may not be obtained through current browser settings.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The ECA prohibits the use of e-mails for advertising purposes without prior, free, specific and informed consent of the addressees. Such consent can be revoked at any time, without any justification or any cost for the addressee.

Conditions for direct marketing by e-mail to corporate subscribers

The sending of direct marketing e-mails does not require consent if they are sent to a legal entity using "impersonal" electronic contact details (e.g. info@company.be). The use of addresses such as john.smith@company.be, however, remains subject to the requirement for prior consent.

Exemptions and other issues

It is permitted to send e-mail for the purposes of direct marketing if the *similar products and services exemption* applies. The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided. The sender must also include the ecommerce information.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Marketing calls to individual subscribers are prohibited in relation to subscribers who object to such marketing calls.

An opt-out list, which is not set forth in the law, has also been put in place on behalf of the industry by the Belgian Direct Marketing Association (the "**BDMA**") in order to enable subscribers to exercise their opt-out right. By signing the so-called "Robinson list", subscribers indicate that they no longer wish to receive direct marketing by mail, e-mail, phone and SMS. BDMA members undertake not to use these subscribers' addresses for marketing purposes anymore.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Non-automated marketing calls to corporate subscribers are prohibited in relation to subscribers who object to such marketing calls.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send direct marketing faxes to individual subscribers without their prior, free, specific and informed consent.

Conditions for direct marketing by fax to corporate subscribers

Direct marketing faxes to corporate subscribers are prohibited in relation to subscribers who object to such marketing faxes.

Exemptions and other issues

No exemptions apply.

Brazil.

Contributed by Lefosse Advogados

General | Data Protection Laws

National Legislation

General data protection laws

There is no specific data protection law in Brazil.

However, other laws ("**Privacy and Confidentiality Laws**") impose a range of privacy obligations that replicate some aspects of a more specific data protection framework. These laws include: (i) the general principles relating to privacy, private life, honour, image and correspondences of individuals and indirect personal data contained in the Brazilian Federal Constitution; (ii) sector-specific laws, such as banking secrecy and telecommunication laws; and (iii) the Criminal Code, which criminalises violation of private computers and interference with private correspondence.

Entry into force

Not applicable.

National Regulatory Authority

Details of the competent national regulatory authority

There is no national regulatory authority in Brazil.

Notification or registration scheme and timing

Not applicable.

Exemptions

Not applicable.

Appointment of a data protection officer

Not applicable.

Personal Data

What is personal data?

Some of the Privacy and Confidentiality Laws are based on a concept of personal data that is similar to the *standard definition of personal data*.

Is information about legal entities personal data?

Yes.

What are the rules for processing personal data?

Since there is no specific data protection legislation, there are no specific rules.

However, the Privacy and Confidentiality Laws apply certain criteria to the disclosure of personal information. Organisations should ensure that: (i) the transfer of personal information to other organisations does not breach confidentiality; and (ii) any party who may have access to that information takes all appropriate measures in order to keep it confidential. Accordingly, organisations are strongly advised to obtain prior written consent before disclosing information about employees, contractors, customers or other third parties (for example, names, addresses, payroll details, photographs, etc.). This includes disclosures to third parties such as outsourced service providers and *data processors*.

Are there any formalities to obtain consent to process personal data?

It is strongly advisable to get consent in writing and preferably in hard copy.

Sensitive Personal Data

What is sensitive personal data?

Despite the lack of specific data protection legislation defining the meaning of "sensitive data" in Brazil, recent case law under the Privacy and Confidentiality Laws does provide a concept of sensitive personal data, namely personal data not related to a person's work or professional activities (such as sexual orientation, race, religion, etc.).

Are there additional rules for processing sensitive personal data?

None in addition to the rules for processing ordinary personal data.

Are there any formalities to obtain consent to process sensitive personal data?

It is strongly advisable to get consent in writing and preferably in hard copy.

Scope of Application

What is the territorial scope of application?

The Privacy and Confidentiality Laws do not contain any express provisions on the territorial effect of data protection laws. It is, therefore, likely to apply to processing of personal data in Brazil and/or processing of personal data which relates to Brazilian citizens or residents regardless of where the organisation carrying out the processing is established.

Who is subject to data protection legislation?

There is no distinction in Brazil between *data controllers* and *data processors*. All persons using personal data need to comply with the Privacy and Confidentiality Laws.

Are both manual and electronic records subject to data protection legislation?

Yes.

Rights of Data Subjects

Compensation

The collection of sensitive data of employees, customers or other third parties may raise claims for compensation for moral damages if the Brazilian Courts consider there is no reasonable business need to collect such information.

Fair processing information

There is no general obligation to provide *fair processing information*.

Rights to access information

Data subjects may obtain their *subject access information* by making a request to the person in charge of the processing. This request is not subject to any formalities (i.e. it can be made by letter, facsimile or e-mail) and in some cases the request can be made verbally.

Objection to direct marketing

A *data subject* is entitled to revoke its consent to the processing of personal data for the purposes of the direct marketing of goods, work or services. The Privacy and Confidentiality Laws do not specify the exact form of any such objection.

Other rights

A *data subject* is entitled to request that an organisation rectifies, blocks or deletes personal data.

Security

Security requirements in order to protect personal data

Brazilian law does not provide for any general requirements in order to protect personal data. However, certain information is protected under sector-specific laws, such as banking secrecy and telecommunication laws.

Specific rules governing processing by third party agents (processors)

The Privacy and Confidentiality Laws apply certain criteria to the disclosure of personal information, including that any party who may have access to that information takes all appropriate measures in order to keep it confidential.

Although not legally required, organisations should consider executing a confidentiality agreement with any person to whom they provide access to others' personal information (whether employees, outsourced service providers or any other third parties). This minimises the organisation's risk exposure in connection with such disclosure.

Notice of breach laws

None.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

For Brazilian legal and constitutional purposes, the geographic location in which data is stored is irrelevant.

Notification and approval of national regulator (including notification of use of Model Contracts)

Not applicable.

Use of binding corporate rules

Not applicable.

Enforcement

Sanctions

Articles 151 to 154 of the Brazilian Criminal Code provide criminal sanctions for violations of privacy in the event of: (i) interference with private or commercial correspondence or interception or violation of telephonic, telegraphic or radio communication, which can result in imprisonment for up to two years (or up to three years if the violator is engaged in activities related to the postal service, telephonic, telegraphic or radio communication); (ii) accessing a private computer without authorization in order to obtain personal advantages or have access to private electronic communication, which can result in imprisonment for up to two years; and (iii) disclosure in breach of duties of secrecy or professional secrecy, which can result in imprisonment for up to one year.

In addition, article 10 of the Brazilian Banking Secrecy Law provides for criminal sanction for violation of banking secrecy, which can result in imprisonment for up to four years.

Note that all sanctions of imprisonment mentioned above will be cumulated with a fine of up to a maximum of approximately BRL 3,000,000.

Breaches of data privacy may also lead to civil and labour liability (i.e. payment of damages).

Practice

Published cases mainly relate to the processing of personal data: (i) by fiscal authorities; (ii) in the telecommunications sector; (iii) by employers; (iv) relating to health and medical matters; and (v) in marketing activities.

Enforcement authority

The Privacy and Confidentiality Laws are enforced by the Brazilian Courts. Enforcement action is also taken by public authorities with regulatory oversight of the consumer, financial and telecoms sectors.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Accessing a person's private computer in order to obtain, modify or destroy personal data, or accessing electronic communication without authorization, whether express or implied, aiming at obtaining personal advantages, may trigger sanctions of imprisonment for up to two years and a fine up to a maximum of approximately BRL 3,000,000. There are no other specific ePrivacy laws.

Cookies

Conditions for use of cookies

No specific cookie laws.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

No specific laws for marketing by email though the general principles in the Privacy and Confidentiality Laws are applicable.

Conditions for direct marketing by e-mail to corporate subscribers

Not applicable.

Exemptions and other issues

Not applicable.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

No specific laws for marketing by telephone though the general principles in the Privacy and Confidentiality Laws are applicable.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Not applicable.

Exemptions and other issues

Not applicable.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

No specific laws for marketing by fax though the general principles in the Privacy and Confidentiality Laws are applicable.

Conditions for direct marketing by fax to corporate subscribers

Not applicable.

Exemptions and other issues

Not applicable.

Bulgaria.

Contributed by Djingov, Gouginski, Kyutchukov & Velichkov

General | Data Protection Laws

National Legislation

General data protection laws

The Personal Data Protection Act implemented the *Data Protection Directive* by being promulgated in the State Gazette, Issue No. 1 of 4 January 2002 and was last amended by the State Gazette, Issue No. 105 of 29 December 2011 (the "**PDPA**").

Entry into force

The PDPA came into force on 1 January 2002.

National Regulatory Authority

Details of the competent national regulatory authority

The Commission for Personal Data Protection (the "**Commission**")
15, Akademik Ivan Evstatiev Geshov Blvd.
Sofia – 1431
Bulgaria

www.cpdp.bg

Notification or registration scheme and timing

In general, any *data controller* must apply for registration with the Commission prior to initiating any personal data processing. The registration covers the *data controller* and the personal data registers controlled by such *data controller* and is free of charge. Hence, if there is any change in the amount, purpose or scope of data processing, the *data controller* must notify the Commission prior to administering such amended registers or implementing such changes in the administered registers, respectively.

The *data controller* may start to process the relevant personal data upon filing the registration application in due manner. The Commission has 14 days in which to accept or reject the registration of the *data controller*.

Exemptions

Exemptions apply in the following situations: (i) *data controllers* operating organised filing systems that are, by virtue of the legislation in force, publicly accessible or accessible only to those who can demonstrate a legitimate interest in obtaining access; (ii) non-profit making organisations carrying out certain processing; (iii) *data controllers* specially exempted by the Commission based on a determination that the processing does not jeopardise the rights and legitimate interests of affected individuals; and (iv) *data controllers* who are natural persons and carry out data processing for personal or domestic purposes.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer under the PDPA.

Personal Data

What is personal data?

The definition of personal data in the PDPA is closely based on the *standard definition of personal data*.

Is information about legal entities personal data?

No. The PDPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the grounds most frequently relied on for personal data processing are the *data subject's* consent, necessary performance under a contract with the *data subject* and compliance with a legal obligation. The legitimate interests condition is not frequently relied upon as grounds for processing non-sensitive data, since the Commission has not yet issued any official opinion regarding the enforceability of this condition.

The PDPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the PDPA.

Are there any formalities to obtain consent to process personal data?

Consent must be informed, specific and express. There are no formalities to obtain consent under the PDPA to process personal data. However, it is recommended for evidential purposes that the consent be in writing.

Sensitive Personal Data

What is sensitive personal data?

Under the PDPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) information about the human genome.

Are there additional rules for processing sensitive personal data?

Processing of sensitive personal data may be initiated only if the *data controller* has obtained an express statement confirming registration with the Commission. The Commission shall issue a statement if after a preliminary inspection the Commission establishes that the data processing will be carried out in conformity with the applicable requirements of the PDPA and in particular the processing complies with the *standard conditions for processing sensitive personal data* as a ground for data processing.

Are there any formalities to obtain consent to process sensitive personal data?

The position is the same as for personal data (see above).

Scope of Application

What is the territorial scope of application?

The PDPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The PDPA applies to *data controllers*. A statutory act may also mandate that an individual, legal entity or state authority shall process personal data and hence shall be a *data controller*. *Data processors* are not subject to the PDPA.

Are both manual and electronic records subject to data protection legislation?

Yes. The PDPA does not differentiate between manual or electronic records. A regulation of the Commission, however, sets forth different obligations for *data controllers* regarding the level of protection and security of personal data depending on whether the records are manual or electronic.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation for any damage suffered as a result of unlawful processing of his/her personal data by a *data controller*. Affected *data subjects* are only entitled to seek compensation for the damages suffered as a result of the acts or actions of the respective *data controller* when such acts and actions are unlawful and, respectively, infringe their legitimate data privacy rights and interests.

Fair processing information

A *data controller* must provide *fair processing information* to *data subjects*. They must also provide information about: (i) recipients or categories of recipients to which the data may be transferred; (ii) the mandatory or voluntary nature of the requested provision of personal data by *data subjects* and the consequences for the *data subjects* in case of refusal to provide requested data; and (iii) the right of *data subjects* to access and correct their collected personal data.

Data controllers are not obliged to provide *data subjects* with such processing information if the respective *data subjects* already have it or the law provides likewise.

If the personal data has been obtained from a third party rather than the *data subject*, there are some exceptions from the obligation to provide processing information (e.g. where it would involve disproportionate effort). Moreover, item (ii) of the above list of *fair processing information* is not required but instead the *data controller* must inform the respective *data subject* about the categories of personal data related to such *data subject*.

Rights to access information

Data subjects may obtain their *subject access information* by written or electronic request to *data controllers*. This right may be exercised at any time and may be exercised free of charge. Where such access may result in the disclosure of data relating to other individuals, the *data controller* must provide the *data subject* with access to only such part of the data as pertains to such *data subject* alone.

Objection to direct marketing

A *data subject* may object by opting out to this effect or require that a *data controller* stops processing data for direct marketing purposes. *Data controllers* must provide *data subjects* with the option of opting out, and if a *data subject* objects to or requires his/her personal data not to be processed for direct marketing purposes, the *data controller* must comply with such a request.

Other rights

Data subjects may obtain from the *data controller* the erasure, correction or blocking of their personal data if processing of those data fails to meet the requirements of the PDPA.

Data subjects may object to the processing of their personal data if there is a legal justification for such objection. *Data subjects* must also be given the opportunity to object to the disclosure of their personal data to third parties.

Data subjects may also require that the *data controller* notify any third parties to whom personal data have been revealed, of any erasure, rectification or blocking of such data.

Security

Security requirements in order to protect personal data

The *data controller* must apply the *general data security obligations*. The Commission regulates in detail the requirements of the *general data security obligations* by a regulation passed to this effect under the PDPA and which became effective as of the end of March 2007. By this regulation the Commission determines the minimum level of technical and organisational measures and the permissible type of security to be provided by a *data controller* to various types of data processing.

Specific rules governing processing by third party agents (processors)

The processing of personal data by a *data processor* must be in accordance with a statutory act, a written contract or other act of the *data controller*, which sets out the obligations of the *data processor*. The *data controller* will be jointly liable for damages caused to third parties resulting from acts or omissions of the *data processor*. The *data processor* may only process personal data in accordance with instructions from the *data controller* unless otherwise directed by law.

In the case of data processing by a *data processor*, it is the *data controller* who is liable for the security measures adopted. It is the obligation of the *data controller* to ensure the *data processor* adopts certain security measures in respect of the processed data.

Notice of breach laws

The PDPA does not provide any obligation for *data controllers* to inform the Commission or *data subjects* of a security breach. The Commission has not issued any guidelines or other directions to this effect.

Specific notice of breach laws apply to the electronic communications sector under the ECA (as defined below) which implements the *Privacy and Electronic Communications Directive*, as amended. The Commission must be notified within three days of the breach being identified.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transfer of personal data outside of the EEA shall only be permissible if the recipient state is able to ensure an adequate level of personal data protection in its territory. *Data controllers*, as data exporters, may not make their own assessment of whether or not the jurisdiction of the data importer provides adequate levels of protection in the case of transborder dataflow. The assessment concerning the adequacy of the level of personal data protection in the recipient state shall be made by the Commission.

Transfers outside of the EEA are also permitted if the *standard conditions for transborder dataflow* are satisfied. Compliance with *binding corporate rules* does not constitute a permissible condition under the PDPA for *transborder dataflows*.

Notification and approval of national regulator (including notification of use of Model Contracts)

In the event of transborder dataflow under the *standard conditions for transborder dataflow*, there is no obligation under the PDPA for the *data controller*, as a data exporter, to obtain the approval of the Commission regarding such transborder dataflow (except where transborder dataflow is made pursuant to *binding corporate rules*).

In the event of transborder dataflow on any other grounds, a *data controller* may carry out transborder dataflow only after receiving the approval of the Commission for the specific transborder dataflow. In this case, to issue the approval, the Commission must first verify the merits of the contemplated transborder dataflow in view of the requirement for an adequate level of protection for *data subjects*.

However, in 2012 the Commission amended its internal regulations of operation and, as a result, changed some rules relating to *transborder dataflows* so that it is necessary for *data controllers* to: (i) undergo verification by the Commission of the merits of the contemplated *transborder dataflows*; and (ii) to obtain the Commission's approval for *transborder dataflows* where the data export is being made: (a) with the consent from the *data subject*; (b) for the performance of a contract with, or in the interest of, the *data subject*; (c) for important public interest grounds, or for legal claims; (d) for the protection of the life or vital interests of the *data subject*; or (e) from a public register. The Commission's regulations of operation take effect as secondary legislation under the PDPA and are unlikely to be upheld by the courts in the case of a dispute between a *data controller* and the Commission. The Commission has not yet made any official statement on these new requirements nor taken formal enforcement action to enforce them.

In all cases of transborder dataflow, regardless of the conditions on which they are carried out, the *data controller* must register the transborder dataflow with the Commission as a change in its effective status as *data controller* (to that of data exporter) prior to initiating such dataflow (unless the *data controller* has already registered its status as a data exporter and the respective transborder dataflow).

Use of binding corporate rules

Although Bulgaria is listed as a member of the mutual recognition club for *binding corporate rules*, the Commission has not issued any statement of approval or recognition regarding the use of *binding corporate rules*.

Enforcement

Sanctions

Administrative sanctions in the form of fines for violations of the PDPA range from BGN 10,000 to BGN 100,000.

Where processing results in a violation of the applicable data protection laws, the Commission has the power to restrict or prohibit the processing of personal data by a *data controller* for a limited period of time and subject to a prior notice to the relevant *data controller*.

The transfer or distribution of computer or system passwords which results in the illegitimate disclosure of personal data constitutes a crime under the Criminal Code, promulgated in the State Gazette, Issue No. 26 of 2 April 1968, last amended by the State Gazette, Issue No. 60 of 7 August 2012, and the penalty for such crime includes imprisonment for up to three years.

Practice

According to the Commission's 2011 Annual Report, in 2011 the Commission approved 42,911 *data controllers*, 28,127 of which were newly registered *data controllers* and the remaining 14,784 updated their existing registrations. The registration applications of *data controllers* regarding sensitive data processing filed with the Commission for 2011 amounted to 1,634. Most of these applications came from *data controllers* occupied in the health care area.

In 2011, the Commission carried out a total of 1,252 on-site examinations. 1,151 of these examinations were of a preliminary control nature and executed in relation to the issuance of approvals for processing of sensitive personal data. In 25 of the on-site examinations, the Commission found non-compliance with the PDPA and took administrative action against the respective *data controllers*.

As a result of the examinations carried out in respect of *data controllers* in 2011, the Commission issued 30 binding directions (compared to only 12 in the previous year). The binding directions covered the following sectors: finance, state administration, public services, transport, media, retail and consumer services and telecommunications. Seven of the issued binding directions were met within the terms determined by the Commission, three were only partially met, and the remaining 20 are still in progress. Subsequent examinations were carried out on some *data controllers* as a result of which no violations were established.

Enforcement authority

The Commission has full supervisory powers over the activity of *data controllers* and is competent to issue binding directions to, and impose fines and restrictions on, *data controllers* for breaches of the PDPA.

Public prosecutors also have enforcement powers but their scope of competence is limited. Public prosecutors usually act on the request of the Commission.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Article 13 of the *Privacy and Electronic Communications Directive* has been implemented by virtue of the Electronic Communications Act (the "**ECA**"), promulgated in the State Gazette, Issue No. 41 of 22 May 2007, last amended and supplemented in the State Gazette, Issue No. 82 of 26 October 2012. The ECA came into force on 26 May 2007.

The rules of the E-Commerce Act, promulgated in the State Gazette, Issue No. 51 of 23 June 2006 (in force since 24 December 2006), last amended by the State Gazette, Issue No. 105 of 29 December 2011, are also of relevance.

Some of the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*, such as the obligation on providers of public electronic communication services to notify the Commission of personal data breaches, have been implemented by virtue of amendments to the ECA, adopted in December 2011. However, other amendments to the *Privacy and Electronic Communications Directive* have not been implemented into Bulgarian national law. For example, the E-Commerce Act has not been amended yet to implement the consent requirements for cookies.

Cookies

Conditions for use of cookies

The E-Commerce Act allows the use of cookies provided that the user has been informed of the use of cookies and he/she has been given the opportunity to refuse the storage of or access to such cookies. Such restrictions are not applicable: (i) to any subsequent use of cookies in so far that the user has not explicitly objected to such use; and (ii) the cookies are used for the sole purpose of carrying out the transmission of a communication over an electronic communication network or for the provision of an information society service requested by the user.

However, the amendments to the *Privacy and Electronic Communications Directive* requiring express consent for the storage of or access to cookies, have not been implemented yet.

Regulatory guidance on the use of cookies

There is no effective regulatory guidance on the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The ECA (Art. 261, para. 1) requires the consent of the individual subscriber as a condition for legally making direct marketing and advertising by e-mail with or without human intervention. Such consent is subject to withdrawal at any time.

Conditions for direct marketing by e-mail to corporate subscribers

Using the defined term "subscriber" to cover legal and natural persons, using or applying for usage of public electronic communications services, the ECA does not differentiate between individual or corporate subscribers with respect to the conditions for legally performing direct marketing by e-mail. Thus, corporate subscribers may be sent direct marketing e-mails only subject to their consent to that effect.

Additionally, pursuant to the E-Commerce Act, the Bulgarian Commission on Consumer Protection keeps a register of the e-mail addresses of legal entities which have expressly opposed receiving unsolicited commercial communication. Sending unsolicited commercial communication to those e-mail addresses, including for direct marketing purposes, is prohibited.

Exemptions and other issues

As an exemption to the rule of the ECA, no prior consent is required for cases where the *similar products and services exemption* applies.

The ECA prohibits direct marketing and advertising e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) the provided opt-out address is not valid.

Pursuant to the E-commerce Act, in case of non-solicited communication, the sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Pursuant to the ECA, direct marketing and advertising by telephone is subject to the same conditions and exemptions as e-mails. Thus, such telephone communications are allowed only subject to the consent of the subscribers. Additionally, a Bulgarian regulation on the rules of issuing of telephone directories expressly provides for the possibility for indexing those subscribers that have expressly consented to receiving unsolicited commercial communications.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Since the ECA does not differentiate between natural and legal entities, the same rules apply with respect to corporate subscribers. Thus, such telephone calls are allowed only subject to the consent of the subscribers. As is the case with individual subscribers, telephone directory indexing is a way, provided for by the law, of expressing consent to receiving unsolicited commercial communications.

Exemptions and other issues

Direct marketing and advertising by telephone is subject to the same exemptions and other issues as marketing or advertising by email.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax is subject to the same conditions and exemptions as e-mails pursuant to the ECA. Thus, such fax calls are allowed only subject to the consent of the subscribers. Additionally, a Bulgarian regulation on the rules of issuing of telephone directories expressly provides for the possibility of indexing those subscribers who have expressly consented to receiving unsolicited commercial communications.

Conditions for direct marketing by fax to corporate subscribers

Since the ECA does not differentiate among natural and legal entities, the same rules apply with respect to corporate subscribers. Thus, such fax communications are allowed only subject to the consent of the subscribers. As is the case with individual subscribers, telephone directory indexing is a way, provided for by law, of expressing consent to receiving unsolicited commercial communications.

Exemptions and other issues

Direct marketing and advertising by fax is subject to the same exemptions and other issues as marketing or advertising by email.

Canada.

Contributed by McCarthy Tétrault LLP

General | Data Protection Laws

National Legislation

General data protection laws

Canada is not an EU Member State and therefore has not implemented the *Data Protection Directive*. However, the Canadian Federal Law Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (the "**PIPEDA**") contains similar provisions to those in the *Data Protection Directive*.

In addition, several Canadian provinces (British Columbia, Alberta, Quebec) have adopted substantially similar data protection laws applicable in the private sector which partly displace PIPEDA in relation to personal information collected within each of these provinces. However, the analysis below is limited to a treatment of the provisions of PIPEDA.

Entry into force

PIPEDA entered partially into force in 2001 and fully into force in 2004.

National Regulatory Authority

Details of the competent national regulatory authority

Office of the Privacy Commissioner
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

http://www.priv.gc.ca

Notification or registration scheme and timing

No. PIPEDA does not contain a registration requirement.

Exemptions

N/A.

Appointment of a data protection officer

Yes. Under PIPEDA, an organisation must make publicly available the name or title, and the address, of the person who is accountable for the organisation's privacy policies and practices and to whom complaints or inquiries can be forwarded.

Personal Data

What is personal data?

"Personal information" is defined in PIPEDA as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation."

This definition is therefore largely similar to the *standard definition of personal data*.

Is information about legal entities personal data?

No, although information about individual partners or individual entrepreneurs may be treated as personal data.

What are the rules for processing personal data?

PIPEDA contains a series of fair information processing obligations that are set out in Schedule 1 to that Act. The principal obligations related to processing personal information are: (i) Identifying Purposes: The purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected (see *fair processing information* below); (ii) Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except as otherwise authorised by law; (iii) Limited Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means; (iv) Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used; and (v) Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Are there any formalities to obtain consent to process personal data?

No. The way in which an organisation seeks consent may vary, depending on the circumstances and the type of information collected. An organisation should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorised representative (such as a legal guardian or a person having power of attorney).

Sensitive Personal Data

What is sensitive personal data?

"Sensitive personal information" is not a legally defined term under PIPEDA. However, some personal information is regarded as being "sensitive" in the non-technical sense and requires additional care. This includes medical records, income records and information about sexual orientation.

Are there additional rules for processing sensitive personal data?

There are no additional rules for processing sensitive personal information under PIPEDA, although the intensity of the obligation may vary depending on the sensitivity of the personal information in question. For example, according to PIPEDA, an organisation should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Similarly, the nature of information security safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information must be safeguarded by a higher level of protection.

Are there any formalities to obtain consent to process sensitive personal data?

No, although an organisation should generally seek express consent when the information is likely to be considered sensitive.

Scope of Application

What is the territorial scope of application?

PIPEDA applies in all provinces and territories in Canada, except to the extent that a province has adopted substantially similar data protection legislation (namely British Columbia, Alberta and Quebec). Even in these latter provinces, PIPEDA applies to the processing of personal information about an employee of an organisation where that organisation collects, uses or discloses such information in connection with the operation of any "federal work, undertaking or business", a legally defined category of undertaking (such as banks, radio broadcasting undertakings, and inter-provincial transportation companies) that is within the legislative authority of the federal Parliament of Canada.

Moreover, a Federal Court has held that, while PIPEDA does not have extra-territorial application, the Canadian Privacy Commissioner has jurisdiction to investigate compliance by a foreign entity as regards its collection and processing of personal information about a Canadian resident.

Who is subject to data protection legislation?

Canadian data protection legislation does not contain the legally defined concepts of *data controller* and *data processor*. In general, the data protection provisions of PIPEDA apply to every organisation in respect of personal information that: (i) the organisation collects, uses or discloses in the course of commercial activities; or (ii) is about an employee of the organisation which the organisation collects, uses or discloses in connection with the operation of any federal work, undertaking or business.

Are both manual and electronic records subject to data protection legislation?

Yes. PIPEDA applies to both manual (paper-based) and electronic records. Specifically, a "record" includes "any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things".

Rights of Data Subjects

Compensation

While individuals do not have a direct right of compensation under PIPEDA, PIPEDA states that a complainant may, after receiving the Commissioner's report or being notified that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in certain specifically identified provisions of PIPEDA. The Court may then, in addition to any other remedies it may give, award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Fair processing information

The purposes for which personal information is collected must be identified by the organisation at or before the time the information is collected.

Rights to access information

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Objection to direct marketing

PIPEDA does not contain specific provisions related to direct marketing. However, an individual may withdraw consent to the collection, use and disclosure of personal information at any time, subject to legal or contractual restrictions and reasonable notice. Moreover, organisations are prohibited from requiring, as a condition of the supply of a product or service, an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes. Generally speaking, therefore, an organisation cannot require an individual to consent to use of personal information for secondary marketing purposes as a condition of receiving the principal service.

Other rights

Organisations may only retain personal information for so long as necessary for the fulfilment of those purposes. An individual may withdraw consent to the collection, use and disclosure of personal information at any time, subject to legal or contractual restrictions and reasonable notice. If an individual withdraws consent to the collection, use and disclosure of personal information and/or if the purpose of collection has been fulfilled, then the organisation should delete such information, in particular where requested by the individual in question.

Security

Security requirements in order to protect personal data

According to PIPEDA, personal information must be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The methods of protection should include: (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organisational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption.

In addition, according to PIPEDA, organisations must make their employees aware of the importance of maintaining the confidentiality of personal information.

Specific rules governing processing by third party agents (processors)

An organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Notice of breach laws

While the Alberta Personal Information Protection Act contains mandatory breach notification requirements applicable within that province, PIPEDA does not currently contain any such explicit requirement. However, a proposed amendment to PIPEDA (not yet in force) may result in the introduction of an express privacy breach notification requirement.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

PIPEDA does not contain any specific restrictions related to cross-border data flows. However, all transfers of personal information to a third party processor, whether within Canada or cross-border, is subject to the "accountability" principle under PIPEDA. Specifically, an organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

Notification and approval of national regulator (including notification of use of Model Contracts)

No. Under PIPEDA it is not necessary to notify or obtain approval from a national regulator for transborder dataflow.

Use of binding corporate rules

PIPEDA does not recognise the concept of *binding corporate rules* as such. However, an organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for

processing. If the information is transferred to another entity within the same corporate group, this is still considered a transfer that is subject to the accountability principle. To the extent that all members of the same corporate group are subject to the same policies related to the protection of personal information and those policies are PIPEDA-compliant, the Privacy Commissioner has accepted that the related parties do not need to put in place a separate data processing agreement as between them in order to comply with the accountability principle.

Enforcement

Sanctions

Under PIPEDA, violations are not subject to administrative fines or sanctions by the Privacy Commissioner. However, a complainant may, after receiving the Commissioner's report or being notified that the investigation of the complaint has been discontinued, apply to a court for a hearing in respect of any matter in respect of which the complaint was made. The Court may then award damages.

Practice

The Privacy Commissioner is primarily interested in encouraging compliance (and does not issue fines). The Privacy Commissioner holds powers of investigation. Specifically, when a privacy complaint is filed against a business, the Privacy Commissioner may choose to investigate the business's data protection practices. Such investigations can be time and resource consuming for the business involved (since the investigations may go beyond a mere review of the business's privacy policies to include a more detailed review of how/whether such policies are implemented in practice). The Privacy Commissioner's decisions are published and several have been widely reported on in the media. Certain cases have led to class actions before the courts.

Enforcement authority

See sanctions summary above.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Canada recently adopted an "anti-spam" law called: "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". It has no official "short title", but is commonly referred to as "Canada's Anti-Spam Law" ("**CASL**"). While it was adopted on 15 December 2010, it is not yet in force. It is expected to come into force early in 2014.

In addition, unsolicited commercial telecommunications (calls, faxes) are regulated under regulations adopted pursuant to the federal Telecommunications Act. Specifically, the Canadian Radio-television and Telecommunications Commission Unsolicited Telecommunications Rules ("**UTR**") have three main components: (i) National Do-Not-Call List ("**DNCL**") Rules creating a registry for consumers; (ii) Telemarketing Rules setting out a basic code of conduct for telemarketing to residential and business consumers; and (iii) Automatic Dialling-Announcing Devices ("**ADAD**") Rules.

Cookies

Conditions for use of cookies

Neither CASL nor the Telecommunications Act specifically regulate the use of cookies. However, PIPEDA's provisions regarding the collection, use and disclosure of personal information (summarised above) apply to cookies to the extent that cookies are used to collect or disclose personal information.

Regulatory guidance on the use of cookies

Not applicable. See above summary of the PIPEDA regulation of the collection, use and disclosure of personal information.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

CASL prohibits businesses from sending commercial electronic messages unless the recipient has given express or implied consent. A "commercial" electronic message is an electronic message where any of its purposes is to encourage participation in commercial activity. An "electronic message" is defined broadly to include any "message sent by any means of telecommunication, including a text, sound, and voice or image message." This definition covers both emails and text messages, for example.

CASL amends the federal Competition Act to prohibit false or misleading representations in the sender description, subject matter field or message field of an electronic message, in the URL or other locator on a webpage.

Conditions for direct marketing by e-mail to corporate subscribers

As regards the above mentioned "consent" requirement, CASL contains a provision pursuant to which a business is deemed to have obtained the requisite "implicit consent" to send a commercial electronic message to any recipient with whom the sender has an "existing business relationship" (as defined in CASL). The above-mentioned prohibitions against false or misleading messages also apply to messages send to corporate subscribers.

Exemptions and other issues

CASL requires that all commercial electronic messages (whether sent to individual or corporate recipients) identify the sender, include the sender's contact information, and provide an unsubscribe mechanism so that the recipient can opt out of receiving future communications.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

If a Canadian business engages in telemarketing it must: (i) register with the National DNCL (even telemarketers who are exempt from the National DNCL Rules must register); (ii) maintain and act in accordance with an internal (not a "national") "do not call" list; and (iii) comply with various rules set out in the UTR, including identifying itself and the purpose of the call to the consumer, and respecting call time limitations. Upon request, a telemarketer must provide a local or toll-free number allowing the customer access to a representative of the telemarketer or, where applicable, its client.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The DNCL Rules do not apply to calls to businesses.

Exemptions and other issues

There are a number of other specific rules concerning telemarketing calls published by the CRTC. These include rules about the times at which calls can be made, the provision of caller line identification, controls over sequential and random diallers and restrictions on silent calls resulting from the use of predictive dialling devices.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

If a Canadian business engages in telemarketing, it must: (i) register with the National DNCL (even telemarketers who are exempt from the National DNCL Rules must register); (ii) maintain and act in accordance with an internal (not a "national") "do not call" list; and (iii) comply with various rules set out in the UTR, including identifying itself, providing a contact fax number and address and respecting call time limitations.

Conditions for direct marketing by fax to corporate subscribers

The DNCL Rules do not apply to calls to businesses.

Exemptions and other issues

There are a number of other specific rules concerning telemarketing calls published by the CRTC. These include rules about the times at which calls can be made, the provision of caller line identification, controls over sequential and random diallers and restrictions on silent calls resulting from the use of predictive dialling devices.

Cyprus.

Contributed by Georgiades & Pelides LLC

General | Data Protection Laws

National Legislation

General data protection laws

The Law on the Processing of Personal Data (Protection of the Individual) of 23 November 2001, Law No. 138(I)/2001, as amended by the Processing of Personal Data (Protection of the Individual) (Amending) Law of 2 May 2003, Law No. 37(I)/2003 and the Processing of Personal Data (Protection of the Individual) (Amending) Law of 11 July 2012, Law No. 105(I)/2012 (collectively, the "**DPA**") implemented the *Data Protection Directive*.

Entry into force

Law No. 138(I)/2001 came into force on 23 November 2001 (except for Sections 9(4) and 9(5) on the free transfer of data to other Member States of the EU, which came into force on 1 May 2004), Law No. 37(I)/2003 came into force on 2 May 2003 and Law No. 105(I)/2012 came into force on 11 July 2012.

National Regulatory Authority

Details of the competent national regulatory authority

Commissioner for the Protection of Personal Data (the "**Commissioner**")
1 Iasonos Street
2nd Floor
1082 Nicosia, Cyprus

www.dataprotection.gov.cy

Notification or registration scheme and timing

Unless an exemption applies, the *data controller* must notify the Commissioner in writing that a filing system is being set up or that processing is to take place. Information notified is kept in the Commissioner's Register of Filing Systems and Processing. Notification should be given to the Commissioner upon the setting up of the filing system, or commencement of processing at the latest. There is no charge for notification. The Commissioner's prior approval is required only when: (i) data are to be transmitted to a country outside the EU; or (ii) two or more filing systems which contain sensitive data or from which data may be retrieved using common criteria are to be interconnected.

Exemptions

The *data controller* must notify the Commissioner unless the processing is exempt. Exemptions apply in respect of processing: (i) necessary for the fulfilment of an obligation imposed by law or by contract under an employment or contractual relationship and the *data subject* has been notified in advance; (ii) relating to customers or suppliers of the *data controller* (except in the case of insurance and pharmaceutical companies, companies that sell information, banks and other financial institutions), provided that the data are not disclosed or transmitted to a third party; (iii) confidentially carried out by lawyers, doctors or health service providers, provided data are not transmitted to third parties (except where necessary in accordance with the client's instructions in the case of lawyers); or (iv) carried out by any organisation (charity, society, company or political party) in relation to its members, provided that the members have consented to the processing and the data are not transmitted to a third party.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. The *Opinion on Personal Data* can be used as guidance on the proper application of the DPA.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities. It therefore applies to information about sole traders to the extent such information relates to the individual trader concerned and to information about partnerships to the extent such information relates to the individual partners.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met.

There are specific exemptions under the DPA for processing for the purposes of taxation, national security, public safety and criminal investigations and prosecutions.

The DPA does not apply to processing by a natural person exclusively for personal or household purposes.

Are there any formalities to obtain consent to process personal data?

The DPA requires that consent must be informed, express, specific and freely given. It is not required that consent is written, but it is more difficult to demonstrate that oral consent has in fact been provided. Obtaining consent from employees can be difficult as it may be hard to demonstrate that consent has been freely given.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) information about criminal prosecutions and convictions.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if any of the *standard conditions for processing sensitive personal data* are met or if: (i) the processing is necessary to serve national needs or for national security reasons; (ii) the data has been publicised by its subject; (iii) the processing is exclusively for statistical, research, scientific and historical purposes provided that, in the Commissioner's view, significant public interest reasons apply and the *data subjects'* rights are duly protected; (iv) the processing is exclusively for journalistic or artistic purposes, provided the right to the protection of privacy and family life is not violated in any way; or (v) the processing is necessary for the protection of public health and the provision of social benefits.

Are there any formalities to obtain consent to process sensitive personal data?

The position is the same as for the processing of personal data (see above).

Scope of Application

What is the territorial scope of application?

The DPA applies a test similar to the *standard territorial test*. However, the DPA will apply to a *data controller* using equipment in Cyprus (other than for transit) regardless of where the *data controller* is established.

Who is subject to data protection legislation?

The DPA imposes obligations on *data controllers*. *Data processors* are not subject to any obligations under the DPA other than the *standard processor obligations*.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to both manual and electronic records which are stored in, or are to be added to, a filing system. A filing system is a structured set of information relating to individuals which has been or may be processed and which is accessible by reference to specific criteria (such as by name or identity card number).

Rights of Data Subjects

Compensation

Data subjects have the right to receive compensation from the *data controller* for damage suffered as a result of breach of the provisions of the DPA, except where it is proven that the *data controller* was not responsible for the event giving rise to the damage.

Fair processing information

A *data controller* must provide *fair processing information* to *data subjects*, as well as the following information: (i) the recipients or categories of recipients of the data; (ii) the existence of rights of access to, and rectification of, data; and (iii) provided this information is necessary to guarantee fair processing, if it is obligatory to provide the data requested and the consequences of a failure to do so. This information must also be provided to *data subjects*: (i) when data are obtained from a third party; and (ii) unless the *data subjects* have already been notified, when data are to be disclosed to a third party for the first time, except where the processing is for statistical, historic or scientific research purposes, it is impossible or requires disproportionate effort or the disclosure of the data is provided for by law, provided, in each case, the Commissioner's permission is obtained.

There is no obligation in the DPA to provide the *fair processing information* and the additional requisite information in any specific language, but such information must be provided in a clear and conducive manner and it may be difficult to demonstrate that this requirement is satisfied unless such information is in a language which the *data subject*

understands. There is no obligation to refer to the DPA itself when providing such information, but such references are usually made when referring to the existence of the rights of access to and rectification of data under the DPA.

Rights to access information

Data subjects may obtain their *subject access information* by request to *data controllers*. *Data controllers* must reply to a subject access request within four weeks and, if requested, include a copy of the relevant personal data (unless providing such personal data involves disproportionate effort). The right to access information is exercised on payment of a fee, to be specified in regulations to be issued by the Commissioner, which is to be repaid to the *data subject* where the *data subject's* request for rectification or erasure of personal data is found to be valid.

Objection to direct marketing

Personal data cannot be processed for direct marketing purposes unless the *data subject's* consent has been obtained in writing. A *data subject* may withdraw their consent to processing of their data for direct marketing purposes.

Such consent need not be obtained where: (i) the service provider was in the possession of such personal data of clients prior to 11 July 2012; (ii) the marketing is for similar goods or services of such provider; (iii) the number of *data subjects* involved is very large; and (iv) the *data subjects* are given the opportunity free of charge to object to such processing (the "**Direct Marketing Exemption**").

Other rights

Data subjects have the right to insist upon rectification, erasure or blocking of data which is incomplete or inaccurate or has been subject to unlawful processing and to receive a free copy of the corrected data. *Data subjects* have the right to object, on compelling legitimate grounds directly relating to a *data subject's* particular situation, to processing of the *data subject's* data which would otherwise be necessary: (i) for the public interest or in the exercise of official authority; or (ii) for the protection of the *data controller's* or recipient's legitimate interests. The right to object is exercised in writing and the *data controller* must reply to the *data subject* within fifteen days.

Data subjects have the right, subject to certain restrictions, to seek a court order suspending or annulling an act or decision taken through data processing intended to evaluate the *data subject's* personality and, in particular, the *data subject's* productivity at work, creditworthiness, credibility and behaviour.

Security

Security requirements in order to protect personal data

The DPA requires compliance with the *general data security obligations*. Processing must be confidential and may be carried out only by the *data controller* and others, upon its instructions and under its control, provided they possess the necessary technical skill and personal integrity.

Specific rules governing processing by third party agents (processors)

Where the processing is carried out by a third party on behalf of the *data controller*, the appointment of the third party must be *by means of a written agreement* and must contain the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any obligation to inform the Commissioner or *data subjects* of a security breach.

Under the ePrivacy Law (see below), a provider of publicly available electronic communication services is under an obligation to promptly give notice containing the specified information to the Commissioner of Electronic Communications and Postal Regulation (the "**Electronic Communications Commissioner**") in the case of a personal data breach.

Where the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider must also promptly give notice to the affected subscriber or individual, containing specified information. However, that notice is not needed if appropriate technological measures have been implemented and applied to the data affected by the breach.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Transborder dataflows can take place if the *standard conditions for transborder dataflow* are satisfied.

Notification and approval of national regulator (including notification of use of Model Contracts)

The Commissioner's permission is required for any transborder dataflow to a third country which is not a *whitelisted country*. Permission is given only if, in the opinion of the Commissioner, the country to which data will be transferred ensures an adequate level of data protection or the transfer satisfies the *standard conditions for transborder dataflow*.

Use of binding corporate rules

Although the DPA does not expressly refer to *binding corporate rules*, it is open to the *data controller* to demonstrate that, by having such rules in place, it provides adequate guarantees for the protection and exercise of the *data subject's* rights. Cyprus is part of the mutual recognition procedure for *binding corporate rules*.

Enforcement

Sanctions

Sanctions are both civil and criminal. Civil sanctions that may be imposed by the Commissioner include a warning and the setting of a deadline for rectifying a breach, fines of up to EUR 30,000, a temporary or permanent withdrawal of the Commissioner's permission and an order to cease processing and/or to destroy data. Criminal sanctions that may be imposed by a court include fines of up to EUR 8,453 and up to five years' imprisonment.

Practice

The Commissioner investigates complaints submitted to his office and also launches his own investigations. Criminal proceedings for contraventions of the DPA have been brought in a limited number of cases and there have been a couple of reported convictions.

The most significant civil sanction imposed by the Commissioner under the DPA to date was a fine of EUR 3,000 and an order to terminate processing and destroy relevant personal data. This was imposed on a company that had infringed section 4(1)(c) of the DPA (the proportionality principle) as more data than necessary was being collected.

In another case, the Commissioner imposed a fine of EUR 2,562 on a company that had infringed various provisions of the DPA, including: (i) Section 15 of the DPA relating to processing for direct marketing purposes, by sending advertising text messages without the prior written consent of the *data subjects*; (ii) Section 5 of the DPA relating to lawful processing; and (iii) Section 7 of the DPA relating to notification to the Commissioner on the setting up of a record or the commencement of processing. The same fine of EUR 2,562 was imposed on the Director - General of a government ministry for breach of Section 10 of the DPA on the security of sensitive personal data.

The most significant civil sanction imposed by the Commissioner under the ePrivacy Law (see below) to date was a fine of EUR 8,000 on a person who had repeatedly infringed various provisions of the ePrivacy Law, specifically: (i) Section 106(1), which prohibited the use of electronic mail for direct marketing purposes without the recipient's prior consent; and (ii) Section 106(5), which required that the sender's identity and a valid electronic mail address, to which a request that communications cease may be sent, be included in such electronic mail.

The first criminal proceeding to be reported related to breach of Section 26(1) of the DPA. It involved the owner of a massage business who had installed a secret video camera without consent of the businesses' clients and without notification to the Commissioner. The sentence imposed at first instance was three months' imprisonment, which was reduced to 55 days on appeal.

In a more recent criminal case, a sentence of 16 months' imprisonment was imposed on an individual for a breach of Section 26(e) of the DPA, which prohibits unauthorised access to, and processing of, personal data. The case involved the unauthorised use of credit card information of other persons for the purpose of illegal money withdrawals.

Enforcement authority

The Commissioner may impose civil (administrative) sanctions on *data controllers* who default on their obligations under the DPA and any other regulatory provisions concerning the protection of personal data processing (such as the ePrivacy Law, which is discussed below). The Commissioner may impose an administrative fine of up to EUR 5,000 on a *data controller* or any person that does not co-operate and/or obstructs an investigation conducted by the Commissioner. The Commissioner has no competence to bring criminal proceedings in court against those who contravene the provisions of the DPA. The Commissioner may report such contraventions to the Office of the Attorney General, who will then decide whether to initiate criminal proceedings.

The Electronic Communications Commissioner may also impose appropriate civil sanctions in respect of non-compliance with the ePrivacy Law (see below).

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Cypriot ePrivacy laws are contained in: (i) an amended Section 15 of the DPA, which came into force on 11 July 2012; and (ii) an amended Part 14 of the Law on the Regulation of Electronic Communications and Postal Services of 30 April 2004, Law No. 112(I)/2004, which came into force on 18 May 2012 (the "**ePrivacy Law**"). The ePrivacy Law has implemented Article 13 of the *Privacy and Electronic Communications Directive*, as amended by the *Citizens' Rights* Directive. The Decree on Legal Persons (Ensuring the Protection of Legitimate Interests with regard to Unsolicited

Communications) of 28 January 2005, No. 34/2005 (the "**Decree**"), which has been issued by the Electronic Communications Commissioner pursuant to the provisions of the ePrivacy Law, came into force on 28 January 2005.

Cookies

Conditions for use of cookies

Under the ePrivacy Law, as amended to implement the *Citizens' Rights Directive*, the use of cookies is allowed only with the consent of the subscriber or user concerned, having been provided with clear and comprehensive information, in accordance with the DPA, on the purposes of the processing. There is an exception if the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or if it is strictly necessary for the provision of an information society service requested by that subscriber or user.

Regulatory guidance on the use of cookies

No guidance is available.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The DPA prohibits the use of an e-mail address for the purpose of marketing, selling goods and offering services from a distance, unless the prior consent of the *data subject* has been obtained in writing. In order to contact the *data subject* for the purpose of obtaining its consent, only personal data relating to the subject which are accessible by the public may be used. Also, the ePrivacy Law provides that electronic mail may be used for direct marketing purposes only where a subscriber who is a natural person has consented to such use in advance.

Conditions for direct marketing by e-mail to corporate subscribers

The Decree provides that the use of e-mail for direct marketing to subscribers who are legal persons is permitted only where a subscriber has clearly declared, in written or electronic form, its willingness to receive such mail to: (i) the sender; (ii) the person responsible for the Cyprus Telephone Directory Database; or (iii) the provider of e-mail services.

Exemptions and other issues

The ePrivacy Law provides that the *similar products and services exemption* shall apply in respect of individual as well as corporate subscribers. Also, the Direct Marketing Exemption (see above) is applicable under the DPA for individual subscribers.

The ePrivacy Law prohibits the sending of emails for direct marketing purposes which: (i) conceal the identity of the sender or person on whose behalf the message is sent; (ii) fail to disclose a valid e-mail address to which the recipient may send a request that communications cease; or (iii) encourage recipients to visit websites that fail to provide the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The DPA prohibits the use of the telephone number of an individual for the purpose of marketing, selling goods and offering services from a distance, unless the individual's prior consent has been obtained in writing. In order to contact the individual for the purpose of obtaining consent, only personal data accessible by the public may be used.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The restrictions on direct marketing by telephone do not apply to corporate subscribers.

Exemptions and other issues

The Direct Marketing Exemption applies (see above).

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The DPA prohibits the use of the fax number of an individual for the purpose of marketing, selling goods and offering services from a distance, unless the individual's prior consent has been obtained in writing. In order to contact the individual for the purpose of obtaining consent, only personal data accessible by the public may be used. The ePrivacy Law provides that a fax number can be used for direct marketing purposes only where the subscriber has consented to such use in advance.

Conditions for direct marketing by fax to corporate subscribers

The Decree provides that the use of a fax number for direct marketing to subscribers who are legal persons is permitted only where the subscriber has clearly declared, in written or electronic form, its willingness to receive such fax messages to: (i) the sender; or (ii) the person responsible for the Cyprus Telephone Directory Database; or (iii) the person who has provided the subscriber with the fax number concerned.

Exemptions and other issues

The Direct Marketing Exemption applies under the DPA for individual subscribers (see above).

Czech Republic.

Contributed by Kinstellar, s.r.o., advokátní kancelář

General | Data Protection Laws

National Legislation

General data protection laws

Act No. 101/2000 Coll., on Personal Data Protection (the "**DPA**") implemented the *Data Protection Directive*.

Entry into force

The DPA entered into force on 1 June 2000 with the exception of the Registration Section, which came into force on 1 December 2000.

National Regulatory Authority

Details of the competent national regulatory authority

Office for Personal Data Protection (*Úřad pro ochranu osobních údaj*) (the "**Office**")
Pplk. Sochora 27,
170 00, Prague 7
Czech Republic

www.uoou.cz

Notification or registration scheme and timing

Personal data may only be processed by a *data controller* that has submitted notification to the Office unless the processing is exempt. If the notification includes all required information and if the Office has not initiated proceedings (the Office will start proceedings in cases where there are serious concerns arising from the notification that the processing could breach the law), the *data controller* may start its data processing activities 30 days after the delivery of the notification to the Office. The notification is not subject to administrative fees.

Exemptions

There is no need to notify the Office of processing if: (i) the data processed are part of public records specifically available in accordance with law, such as the Companies Register or a certain part of the Trade Licences Register; (ii) the *data controller* needs to process the data in order to benefit from the rights arising, or fulfil the obligations under, specified legislation (this relates, in particular, to data processed in the course of judicial resolution of disputes, to a number of fields of administrative decision-making, to employers' duties under the Employment Act and accounting and social security legislation); or (iii) political parties or non-profit-making organisations process personal data concerning their members or partners and such data are not disclosed without the consent of such members or partners.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data* and is interpreted broadly. It includes any information which can lead to the direct or indirect identification of an individual. According to the guidance issued by the Office in 2001, the definition of personal data cannot be considered in isolation, it should be interpreted in light of concrete circumstances of personal data processing.

The Supreme Administrative Court ruled in 2008 (decision 9 As 34/2008-68) that a mobile phone number constitutes personal data even if it is not accompanied by the name and/or address of an individual, because the person can be contacted and subsequently identified. The fact that the individual may have had the mobile phone number only temporarily is irrelevant.

Is information about legal entities personal data?

No. The DPA does not apply to data relating to legal entities. However, data relating to legal entities are also protected by national legislation, in particular, by the provisions of the Commercial Code relating to business names and unfair competition. Information about sole traders and partnerships is personal data as they are treated as individuals.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. The legitimate interests condition may only be relied upon if the processing is not in contradiction to the *data subject's* right to personal and private life.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

There are no formalities under the DPA to obtain consent to process non-sensitive personal data. Consent can be express, written, oral or implied. The *data controller* must be able to provide evidence of the *data subject's* consent during the entire period of data processing. Obtaining consent from employees can be difficult as, in some cases, it may be hard to demonstrate that consent has been freely given by the employee.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes: (i) the *standard types of sensitive personal data*; (ii) information about criminal offences and alleged criminal offences; and (iii) biometric and genetic data.

Are there additional rules for processing sensitive personal data?

Personal data may be processed if the *standard conditions for processing sensitive personal data* are met.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be express and the *data controller* must be able to prove the *data subject's* consent during the entire period of data processing. Obtaining consent from employees to process their sensitive personal data can be difficult (see above).

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The DPA applies mainly to *data controllers*. However, *data processors* are directly subject to the security obligations. The DPA does not apply to data processing performed by an individual exclusively for personal needs. In addition, the DPA does not apply to casual personal data collection, provided that the data are not processed any further.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to both manual and electronic records and the criteria for processing both types of record are identical.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation if they suffer damage or damage and distress.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects* including information about *data subjects'* rights. If the data are obtained from a *data subject*, the information provided must also include a note as to whether the *data subject* is required by law to provide the requested personal data or whether the provision of such data is voluntary.

There is no obligation in the DPA to provide this information in Czech, though it may be difficult to show that the information has been fairly provided if it is not provided in a language the *data subject* is familiar with.

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. The *data controller* is entitled to ask for reasonable payment not exceeding the costs associated with the provision of a response to a subject access request.

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing data for direct marketing purposes. The *data controller* must cease processing immediately after the receipt of such request.

Other rights

The *data subject* may ask the *data controller* to correct his personal data if they are untrue or inaccurate. The *data subject* is entitled to ask the *data controller* to inform him which of his personal data are being processed.

If the *data subject* discovers that the *data controller* or *data processor* has breached its duties, he may: (i) ask the Office to take remedial measures; (ii) request that the *data controller* or *data processor* refrain from such activity; (iii) request that the data are corrected, completed, blocked or destroyed; or (iv) request a financial remedy.

Security

Security requirements in order to protect personal data

The *data controller* (as well as the *data processor*) must comply with the *general data security obligations*. The DPA refers only to the *general data security obligations* and does not contain any specific security requirements.

The *data controller* (or the *data processor*) must develop and document technical and organisational measures it implements and perform its own risk assessment in relation to the: (i) fulfilment of data processing instructions by persons who have immediate access to the personal data; (ii) prevention of unauthorised persons' access to personal data; (iii) prevention of unauthorised reading, creating, copying, transferring, modifying or deleting of records containing personal data; and (iv) measures enabling determination and verification of to whom the personal data were transferred.

Specific rules governing processing by third party agents (processors)

Authorisation of the *data processor* arises either from a special act or is based on a written agreement with the *data controller* on whose behalf the data are processed. The agreement must include the extent and purpose of the data processing and the period for which it is conducted and an obligation to comply with the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any obligation to inform the Office or *data subjects* of a security breach. However, *data controllers* in certain sectors may be required to inform special sectorial regulators of any breach (for example, financial services firms may be required to report any security breach).

Act No. 127/2005 Coll., on electronic communications and on amendment to certain related acts (the "Electronic Communications Act") sets out specific rules on a notice of a breach for the electronic communications sector. In the event of a breach of personal data protection, the provider of the electronic communication service is obliged to notify the Office without undue delay. The notification shall include a description of the consequences of the breach and the technical measures that the provider has implemented or suggests be implemented. The Office may also instruct the provider to notify the *data subject* in question if the provider has not already done so.

If there is a risk that: (i) the breach will substantially affect the privacy of the *data subject*; or (ii) the provider has not implemented sufficient measures, then the provider has to notify both the Office and the relevant *data subject* of this.

Providers must keep a record of all such breaches, including descriptions of the consequences and implemented measures.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the *standard conditions for transborder dataflow* or the country of destination is party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108).

Notification and approval of national regulator (including notification of use of Model Contracts)

The *data controller* must apply for the Office's approval prior to the transfer unless the transfer is based on the *Model Contracts*, to a *whitelisted country* or to a country that is party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Use of binding corporate rules

The Czech Republic is part of the mutual recognition club for *binding corporate rules* and the Office is generally open and favourable to the use of *binding corporate rules*. So far, the Office has not been asked to act as main approving authority, as multinational companies that wish to implement the *binding corporate rules* usually have their headquarters outside of the Czech Republic and as such they approach other regulators to lead the process.

Enforcement

Sanctions

Sanctions and penalties under the DPA: If legal entities, or individuals undertaking business under special laws, breach, as *data controllers* or *data processors*, any of the obligations in the DPA, they may be required to pay a penalty of up to CZK 5,000,000. If legal entities breach duties related to sensitive data processing or if the breach endangers the privacy and private life of more people (the number of people depends on the context of the case, in practice this involves dozens

of people or more), they may be required to pay a penalty of up to CZK 10,000,000. Legal entities are not responsible for the breach if they prove that they have made every possible effort to prevent the breach of the legal obligation.

If individuals, as *data controllers* or *data processors*, breach any of the obligations in the DPA, they may be required to pay a penalty of up to CZK 1,000,000. If individuals breach duties related to sensitive data processing or if the breach endangers the privacy and private life of more people, they may be required to pay a penalty of up to CZK 5,000,000.

In addition, if a person who is employed by or works for a *data controller* or *data processor* or who, in the course of fulfilling his rights and obligations imposed by law, comes into contact with the personal data of the *data controller* or the *data processor* and breaches the confidentiality duty under the DPA, he may be subject to a fine of up to CZK 100,000.

If individuals, legal entities, or individuals undertaking business under special laws, breach the prohibition to publish the personal data protected by special laws, they may be required to pay a penalty of up to CZK 1,000,000. If such breach is committed by press, film, radio, television, publicly available computer network or by equally effective way, they may be required to pay a penalty of up to CZK 5,000,000.

There are also sanctions under the Criminal Code. Under current regulations, only individuals are liable for the criminal offence of the unauthorised disclosure of personal data. This offence has no relevance to *data controllers* which are legal entities. However, their employees may be held liable for such criminal offence and may be punished by a term of imprisonment of up to eight years, prohibition of professional activities or a fine.

Practice

The Office conducted 179 new inspections in 2011. 144 prosecutions were closed in 2011. Typically, the level of penalty imposed is in the tens of thousands of CZK but is rarely over CZK 200,000. The highest penalty levied to date was CZK 2,300,000 in 2009. In this case, the State Institute for Drug Control unlawfully collected and processed personal data in connection with drug distribution.

Enforcement authority

The fines for breaches of the DPA are imposed by the Office. If not paid, fines are enforced by the competent customs authority. Sanctions under the Criminal Code are imposed by the criminal courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Act No. 480/2004 Coll., on Certain Information Society Services (the "**ECA**") implemented Article 13 of the *Privacy and Electronic Communications Directive* in the Czech Republic.

The ECA has been amended to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Cookies are regulated by the Electronic Communications Act. Under the Electronic Communications Act, there is no requirement to obtain the user's consent for the use of a cookie. Currently, it is only necessary to inform the users of the use of cookies and offer them the right to refuse their use (i.e. the opt-out principle). Such obligation does not apply if the cookie is strictly necessary for the provision of a service to the user. This remains the same even after the Electronic Communications Act was amended (i.e. the opt-in principle required by the *Privacy and Electronic Communications Directive* is not reflected in the latest amendment to the Electronic Communications Act). In addition, the Electronic Communications Act does not expressly refer to the use of browser settings as a means to obtain consent.

Regulatory guidance on the use of cookies

There is no regulatory guidance for the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under the ECA, direct marketing e-mail may only be sent to individuals with their prior consent.

Conditions for direct marketing by e-mail to corporate subscribers

Under the ECA, direct marketing e-mail may only be sent to legal entities with their prior consent.

Exemptions and other issues

It is permitted to send e-mail for the purposes of direct marketing if the *similar products and services exemption* applies. The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; (ii) the e-mail is not clearly and distinctly identified as commercial communication; or (iii) an opt out address is not provided.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to individual subscribers without their consent.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to corporate subscribers without their consent.

Exemptions and other issues

Calls can be made to subscribers if the telephone number is mentioned in the public telephone directory and if the public telephone directory does not include a note that the subscriber does not wish to be contacted for marketing purposes.

Calls can be made to existing customers if they do not object to it.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send direct marketing messages to individual subscribers by fax without their consent.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send direct marketing messages to corporate subscribers by fax without their consent.

Exemptions and other issues

If the fax number is mentioned in the public telephone directory and if the public telephone directory does not include a note that the subscriber does not wish to be contacted for marketing purposes, then it is possible to send direct marketing messages by fax to such subscriber.

Marketing messages can be sent to existing customers if they do not object to it.

Denmark.

Contributed by Gorrissen Federspiel

General | Data Protection Laws

National Legislation

General data protection laws

The Act on Processing of Personal Data, Act No. 429 (the "**DPA**") dated 31 May 2000 (as amended by: section 7 of Act No. 280, dated 25 April 2001; section 6 of Act No. 552, dated 24 June 2005; section 2 of Act No. 519, dated 6 June 2007; Act No. 188, dated 18 March 2009, section 2 of Act No. 503, dated 12 June 2009 and section 1 of Act no. 1245 dated 18 December 2012) implementing the *Data Protection Directive*.

Entry into force

The DPA entered into force on 1 July 2000.

National Regulatory Authority

Details of the competent national regulatory authority

The Data Protection Agency (*Datatilsynet*) (the "**Agency**")
Borgergade 28, 5
DK-1300
Copenhagen K
Denmark

www.datatilsynet.dk

Notification or registration scheme and timing

Data controllers need to notify the Agency of any processing though there are exemptions for many types of routine processing that do not involve sensitive or semi-sensitive data, i.e. criminal offences, serious social problems and other purely private matters than those covered by the *standard conditions for processing personal data*.

In addition, *data controllers* must obtain prior permission from the Agency for the following data processing: (i) processing of sensitive or semi-sensitive data; (ii) processing undertaken for the purpose of warning others against business relations with, or employment of, a *data subject*; (iii) processing undertaken by a credit information bureau for the purpose of disclosing, as part of its business, data for the evaluation of financial soundness and creditworthiness; (iv) processing undertaken for the purpose of commercial employment assistance; (v) processing undertaken solely for the purpose of supplying legal information; or (vi) certain transfers of data to a third country, including, in some cases, transfers based on *Model Contracts* (see below). A fee of DKK 2,000 is payable for an application for permission to process data.

Further, credit information agencies or *data processors*, which are information technology service providers, are required to notify the Agency prior to initiating processing of personal data in Denmark.

Exemptions

No prior permission or notification is required for other processing activities.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*.

If it is in any way possible to establish a connection between the information and specific *data subjects*, the data will be considered personal data under the DPA. For instance, if data has been made anonymous or encrypted and there exists a code to de-anonymise or decrypt the data, then the data is still considered personal data. However, if the data has undergone processing following which it is no longer possible in any way to link data to the *data subject*, such data will not be considered personal data within the meaning of the DPA. According to Danish case law, IP addresses are considered personal data.

The Agency has not published any guidelines regarding the definition of personal data.

Is information about legal entities personal data?

No. The rules on processing of personal data in the DPA only apply to the processing of data concerning private individuals, small personally-owned private companies and small partnership companies. Information concerning a corporation as such is not considered personal data. However, information on employees of a company falls within the definition of personal data.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the legitimate interest condition is frequently relied upon as the ground for processing non-sensitive personal data.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

No. It is not a requirement to obtain consent from the *data subject* in writing; however, the consent must be freely given, specific and informed and, in order for the *data controller* to be able to prove that such consent has been obtained, it is recommended that the consent is obtained in writing. Due to the fact that the consent must be freely given, specific and informed, an implied consent or a consent obtained by an "opt-out" solution will not fulfil the requirements to obtain consent under the DPA.

Consent from employees is to be obtained in the same manner as consent is obtained from any other *data subjects*.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data means the *standard types of sensitive personal data*.

In addition, the DPA defines semi-sensitive data as criminal offences, serious social problems and purely private matters other than those covered by the *standard conditions for processing personal data*. Private sector *data controllers* may process such data only in certain circumstances. Data of a purely private nature is subject to additional rules set out below.

According to the guidelines from the Agency, biometric information is considered personal data and the processing of biometric information is governed by the DPA. Consequently, the *data controller* must consider: (i) the necessity of the use of biometric information; and (ii) whether the objective of the processing may be obtained by other less radical means. The *data controller* is obliged to evaluate whether the biometric system fulfils the requirement of objectivity and proportionality in the DPA. In addition, biometric information is considered to be sensitive personal data if the information concerns the health of an individual.

Finally, the DPA contains specific rules on the processing of Danish social security numbers. The processing of these identification numbers are subject to the additional rules set out below.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may, as a main rule, be processed if the *standard conditions for processing sensitive personal data* are met. Also, sensitive data may be processed where the processing of data takes place for reasons of substantial public interest. The Agency shall give its authorisation in such cases and the processing may be made subject to specific conditions. The Agency shall notify the Commission of any derogation.

Private sector *data controllers* may process semi-sensitive data only in certain circumstances. Such data may only be processed or transferred to a third party with: (i) the explicit consent of the *data subject*; or (ii) if such transfer is for the purpose of public or private interests that clearly outweigh the interests of the *data subject*. Specific provisions apply to the public sector's processing of semi-sensitive data. Private sector *data controllers* may process information on identification numbers where: (i) this follows from law or regulations; (ii) the *data subject* has given his explicit consent; (iii) the processing is carried out solely for scientific or statistical purposes; (iv) it is a matter of disclosing an identification number and such disclosure is a natural element of the ordinary operation of companies of the type mentioned and the disclosure is of decisive importance for an unambiguous identification of the *data subject*; or (v) the disclosure is demanded by an official authority.

Are there any formalities to obtain consent to process sensitive personal data?

No. The position is the same as for the processing of personal data (see above).

Scope of Application

What is the territorial scope of application?

The DPA applies to the processing of data undertaken for a *data controller* established in Denmark, provided that the activities take place within the EU, and to processing undertaken for Danish diplomatic offices.

The DPA also applies to *data controllers* established in a third country: (i) if the collection of data in Denmark is undertaken for the purpose of processing in a third country; or (ii) if the processing is undertaken through means located in Denmark, unless such means are only used for the purpose of sending data through the territory of the EU, in which case the *data controller* must designate a representative established in Denmark and provide written notification of the details of the representative to the Agency. A "third country" is defined in the DPA as a country which is not a Member State of the EU and which has not implemented agreements with the EU that contain provisions similar to the provisions of the *Data Protection Directive*.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. *Data processors* are not directly subject to the DPA. However, the provisions in the DPA regarding security apply to *data processors* and the Agency may issue prohibitions or mandatory injunctions against *data processors* in special cases.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to all electronic records and to manual records to the extent that these are, or will be, contained in a filing system. A filing system is defined in the DPA as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Rights of Data Subjects

Compensation

The *data controller* shall compensate any damage caused by the processing of data in violation of the provisions in the DPA unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data. As such the liability of *data controllers* under the DPA is similar to the ordinary liability for damages under Danish law.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. Such information must also include the category of any recipients of the data, whether answering questions is compulsory or voluntary and the possible consequences of failing to answer, and information regarding rights of access and rectification.

If personal data are not obtained from the *data subject*, the same information must be provided to the *data subject* on collection of the data, unless the *data subject* is already aware of the information or if providing it proves to be impossible or would involve disproportionate effort.

The *fair processing information* is not required to be given in Danish and, for private *data controllers*, it is not required to make reference to the DPA.

Rights to access information

Data subjects may obtain their *subject access information* request to *data controllers*. Where personal data relating to the *data subject* is being processed, the *data controller* must inform the *data subject* of the data being processed, the purposes of the processing, the categories of the recipients of the data and any available information as to the source of such data.

The *data controller* must reply to the request without delay. If the request has not been replied to within four weeks from the receipt of the request, the *data controller* must inform the *data subject* of the grounds for this and of the time at which the decision can be expected to be available.

According to executive order No. 533 of 15 June 2000, a private *data controller* may require a payment of DKK 10 per page only in the event that the *data subject* has requested the information be provided to him in writing. However, the payment shall never exceed DKK 200. In the event that an individual has requested the *data controller* to confirm in writing that the private *data controller* does not process any personal data about him, the *data controller* may require a payment of DKK 10.

In the event that the *data subject* has not requested the confirmation or the information above in writing, the private *data controller* cannot require any payment.

Objection to direct marketing

A *data subject* may require that a *data controller* stop processing data for direct marketing purposes.

Other rights

Data subjects may object to the processing where justified.

The *data controller* shall at the request of the *data subject* rectify, erase or block data which is inaccurate or misleading or in any other way processed in violation of law or regulations.

In certain cases, a *data subject* may object to decisions being taken about him based solely on electronic processing.

Security

Security requirements in order to protect personal data

The DPA requires that *data controllers* apply the *general data security obligations*. The Agency has issued guidelines which deal with OCES certificates and the security in connection with transmission of personal data via the internet in the private sector. The Agency requires that confidential information and information which is deemed confidential is encrypted when the information is sent via webpages. Further, the Agency recommends that a strong encryption is used if sensitive or confidential data is being sent via e-mail.

The public administration is subject to statutory order No. 528 of 15 June 2000 which sets out security requirements for the processing of personal data in the public administration.

Specific rules governing processing by third party agents (processors)

All processing by a *data processor* must be subject to a written agreement between the *data controller* and the *data processor*. The agreement must contain the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any obligation to inform the Agency or *data subjects* of a security breach.

However, in practice, the Agency has interpreted the obligation to comply with good practices of processing data as requiring a *data controller* to notify *data subjects* of any unintended publication of personal data on the internet and ensure that such personal data are removed from publicly available search engines. In particular cases, the Agency has held it as a breach of good practice where *data subjects* were not notified personally.

Additionally, *data controllers* in certain sectors may be required to inform sector regulators of any security breach (for instance, financial service firms may be required to inform the Danish Financial Authority of any such breach).

Specific notice of breach requirements will also apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. The amendments have been implemented into Danish law by the Act on Electronic Communications and Services no. 169 of 3 March 2011 and Executive Order no. 445 of 11 May 2011.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA prohibits transfer outside of the EEA unless the destination ensures adequate protection for the data. In addition, the Agency may grant permission for the transfer of data (which may be conditional), if the *data controller* provides satisfactory guarantees for the protection of the rights of the *data subjects*, by way of example, if the transfer of personal data outside of the EEA is based on the standard conditions in the *Model Contracts*.

Notification and approval of national regulator (including notification of use of Model Contracts)

The EU Commission's approval of the standard contractual clauses is binding on the Agency. From 1 January 2013 it is no longer necessary to obtain the Agency's approval for transfers based on the Commission's Model Contract provided that the Model Contract remains in its original wording. If the Model Contract is amended then approval from the Agency is required.

If the contemplated transfer does not take place based on the standard contractual clauses, the application for approval will be subject to perusal by the Agency.

Use of binding corporate rules

The Agency has approved the use of *binding corporate rules* in Denmark.

There have only been a few cases before the Agency on *binding corporate rules*. One of them was a case where *binding corporate rules* were filed by General Electric and approved by the Agency, which was not the coordinating authority. Prior to this approval, General Electric's *binding corporate rules* had already been approved in the UK, Germany, Belgium and Ireland. Another approval was given by the Agency in 2011 in relation to Accenture A/S and in 2012 to Novo Nordisk A/S.

Further, the Agency is currently assisting a number of Danish companies in the preliminary preparations of *binding corporate rules* in which the Agency will be the coordinating authority.

Enforcement

Sanctions

Any person or legal entity that commits an offence under the DPA is liable upon conviction to a fine or imprisonment of up to four months.

Practice

The number of new cases handled by the Authority in 2011 was 5,442 – a small decrease of 4 per cent from the 5,665 cases handled in 2010, which also includes preparatory work in connection with new regulations. The number of cases initiated by the Agency after complaints from citizens against companies was 1,235 in 2011 compared to 1,296 in 2010. The number of cases initiated by the Agency itself was 96 (including 60 inspections, of which 37 were related to private companies). 176 new international cases were registered in 2011.

The Agency does not publish an inventory of prosecutions. However, to our knowledge there have been the following court cases: (i) a municipality had transferred sensitive personal data concerning a former employee to another municipality, and this was found to be illegal according to the DPA. The transferring municipality was ordered to pay EUR 3,330 in tortious compensation to the employee. The case was confirmed in 2011 by the Danish Supreme Court and this was the first time the Supreme Court had been asked to assess and interpret the DPA; (ii) a criminal court case from 2010 in which the defendant was found not guilty of violating the DPA by publishing CCTV footage of a robber; (iii) in a court case from 2008 an employer was ordered to pay EUR 3,360 in tortious compensation to an employee due to unjustified TV surveillance in violation of the DPA; (iv) a court decision in 2007 resulted in a fine of approximately EUR 400 for publishing the social security numbers of two individuals on a website for seven days; and (v) in a court case in 2007, an employer was ordered to pay EUR 1,333 in tortious compensation to an employee because the employer had violated the DPA by publishing personal data of the employee on the internet.

In 2007, the Agency issued an order to stop the publication and disclosure of videos from surveillance cameras showing recognisable individuals to anyone besides the police. The video in question had been posted on the internet and showed a burglar caught in the act. The video was accompanied by a message that anyone who could identify the perpetrator would receive a reward.

So far only fines have been levied. The highest fine imposed to date amounted to approximately EUR 6,500 and was imposed in 2001. The case concerned the unauthorised transfer of the customer database of a newspaper to another newspaper, which used the customer database for marketing purposes. The case did not go to court as the newspaper accepted the fine.

Enforcement authority

The Agency has no power to take enforcement action in Denmark, other than to issue enforcement notices. Crucially, the Agency has no ability to fine organisations itself but can request that the Danish Public Prosecution Office instigate proceedings.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Article 13 of the *Privacy and Electronic Communications Directive* regarding unsolicited direct marketing has been implemented by Act No. 450 of 10 June 2003, that came into force on 25 July 2003, which amended Section 6a (now Section 6) of the Marketing Practices Act (no. 58 of 20 January 2012). The *Privacy and Electronic Communications Directive* as amended by Directive 2009/136/EF of 25 November 2009 has been implemented by the Danish Act on Electronic Communications and Network Services no. 169 of 3 March 2011.

Cookies

Conditions for use of cookies

The Danish Executive Order on Cookies no. 1148 of 9 December 2011 entered into force on 14 December 2011. Guidance to the Executive Order was published in December 2011 by the supervisory authority – The Danish Business Authority.

The Executive Order requires prior specific and informed consent for the use of cookies unless: (i) the storage has the sole purpose of carrying out communications via an electronic communications network; or (ii) the cookie is strictly necessary for the provision of a service to a user and the user has specifically requested such service.

The consent of the user to the storing of cookies can be either an implied or active consent. However, as the Danish Business Authority has not yet made any decisions on the interpretation of the Executive Order many issues remain unclear, especially in relation to this issue of technical and practical measures to obtain consent from the user.

Currently, it is necessary to inform users of the use of cookies, the purpose of such use, the duration of the cookies and the name of the entity/person storing the cookies, and the users should be offered the right to refuse the use of cookies. The information provided must be deemed clear and sufficient.

Regulatory guidance on the use of cookies

The Danish Executive Order was originally due on 25 May 2011 and the delay was a result of the fact that the consultation period raised many questions and issues, which still need further clarification and discussions within the relevant authority and the industrial and professional associations.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

It is not permitted to transmit unsolicited direct marketing e-mail (as well as SMS and MMS messages), unless the recipient has notified the sender of his consent to such communications.

Conditions for direct marketing by e-mail to corporate subscribers

It is not permitted to transmit unsolicited direct marketing e-mail (as well as SMS and MMS messages), unless the recipient has notified the sender of his consent to such communications.

Exemptions and other issues

It is permitted to send e-mails for the purposes of direct marketing if the *similar products and services exemption* applies. In this regard, the use of premium-rate telephone numbers or SMS messages as the means to object is not permitted.

Notwithstanding the above, the Marketing Practices Act prohibits direct marketing e-mails from being sent if: (i) the person concerned has declined such communications; (ii) it appears from a list prepared each quarter by the Central Office of Personal Registration (the "**CPR**") that the person concerned has declined communications for such marketing purposes; or (iii) the sender, by consulting the CPR, has become aware that the person concerned has declined such communication. The sender must also include the information in the Act on E-commerce (Act no. 227 of 22 April 2002*)* to the extent that the e-mail concerns information society services covered by the Act.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make unsolicited direct marketing calls to individual subscribers unless the subscriber has notified the caller of his consent to this approach.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is permitted to make unsolicited direct marketing calls to corporate subscribers.

Exemptions and other issues

It is permitted to make unsolicited direct marketing calls to an individual subscriber (consumer) if the call concerns: (i) the ordering of books; (ii) the taking out of a subscription to a newspaper, a magazine or a gazette; (iii) the procurement of insurance contracts; or (iv) the subscription to certain kinds of rescue assistance services (for example, a roadside assistance subscription) or the transport of patients.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send unsolicited direct marketing faxes to individual subscribers unless the recipient has notified the sender of their consent to such communications being sent.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send unsolicited direct marketing faxes to corporate subscribers unless the recipient has notified the sender of their consent to such communications.

Exemptions and other issues

No exemptions apply.

Dubai International Financial Centre.

General | Data Protection Laws

National Legislation

General data protection laws

The DIFC Data Protection Law 2007 (DIFC Law No. 1 of 2007) (the "**Data Protection Law**") and the DIFC Data Protection Regulations (the "**Regulations**").

Entry into force

The DIFC Data Protection Law 2007 (DIFC Law No. 1 of 2007) was issued on 6 January 2007. The DIFC Data Protection Regulations were issued by the DIFC Authority Board on 15 February 2007.

National Regulatory Authority

Details of the competent national regulatory authority

Dubai International Financial Centre Authority

Level 14, The Gate
PO Box 74777
Dubai
United Arab Emirates

Email: administration@dp.difc.ae

http://www.difc.ae

The DIFC Authority is responsible for administering the Data Protection Law. The President of the DIFC is charged with appointing the Commissioner for Data Protection (the "Commissioner") to administer the Data Protection Law on behalf of the DIFC Authority.

Notification or registration scheme and timing

The Data Protection Law does not generally require notification in respect of the processing of personal data.

However, a *data controller* must notify the Commissioner where any personal data processing operation or set of operations occurs, involving: (i) the processing of sensitive personal data; or (ii) the transfer of personal data to a recipient outside the DIFC which is not subject a data protection regime which ensures an "adequate" level of protection (see *Restrictions on transfers to third countries*, below). Notification by a *data controller* is carried out by completing a notification form and sending it to the Commissioner at the DIFC Authority.

Exemptions

No.

Appointment of a data protection officer

There is no obligation to appoint a data protection officer.

Personal Data

What is personal data?

The Data Protection Law defines personal data as any information relating to an identifiable natural person. An identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity.

The definition is therefore substantially similar to the *standard definition of personal data*.

Is information about legal entities personal data?

Personal data is any information which relates to an identifiable natural person. Consequently, information relating to a partnership or sole trader could be considered personal data where such information relates to identifiable natural persons (such as partners, owners, employees or customers of the relevant legal entity).

What are the rules for processing personal data?

Personal data may only be processed if: (i) the *data subject* has given his written consent to the processing of that personal data; (ii) the processing is necessary for the performance of a contract to which the *data subject* is party or in order to take steps at the request of the *data subject* prior to entering into a contract; (iii) processing is necessary for compliance with any legal obligation to which the *data controller* is subject; (iv) processing is necessary for the performance of a task carried out in the interests of the DIFC, the Dubai Financial Services Authority, the DIFC Court or in the exercise of the Commissioner's functions or powers vested in the *data controller* or in a third party to whom the personal data is disclosed; or (v) processing is necessary for the purposes of the legitimate interests pursued by the *data controller* or by the third party or parties to whom the personal data is disclosed, except where such interests are overridden by compelling legitimate interests of the *data subject*.

These conditions are therefore substantially similar to the *standard conditions for processing personal data*.

Are there any formalities to obtain consent to process personal data?

Consent, if required, must be given in writing.

Sensitive Personal Data

What is sensitive personal data?

Sensitive personal data is personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade union membership and health or sex life.

The definition is therefore substantially similar to the *standard types of sensitive personal data*.

Are there additional rules for processing sensitive personal data?

Sensitive personal data should not be processed unless conditions substantially similar to the *standard conditions for processing sensitive personal data* are satisfied or certain other conditions, mainly related to banking or financial services, are satisfied.

These other conditions include where: (i) processing is necessary to uphold the legitimate interests of the *data controller* recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by the legitimate interests of the *data subject*; (ii) processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or obligations relating to the prevention or detection of any crime that apply to a *data controller*; (iii) processing is required to protect members of the public against financial loss due to dishonesty or other seriously improper conduct by persons concerned in the provision of certain financial services; or (iv) processing is authorised in writing by the Commissioner.

Are there any formalities to obtain consent to process sensitive personal data?

Consent, if required, must be given in writing.

Scope of Application

What is the territorial scope of application?

The Data Protection Law applies in the jurisdiction of the Dubai International Financial Centre and is therefore applicable to all DIFC entities, both regulated and non-regulated by the DFSA.

Who is subject to data protection legislation?

The Data Protection Law applies to the activities of *data controllers* and *data processors*, as well as persons acting under *data controllers* and *data processors*.

Are both manual and electronic records subject to data protection legislation?

Yes.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation where they have suffered damage by reason of any contravention by a *data controller* of any requirement of the Data Protection Law or the Regulations.

Fair processing information

Upon commencing collection of personal data in respect of a *data subject*, *data controllers* must provide *data subjects* with *fair processing information*, which should include, amongst others things: (i) information detailing the recipients or

categories of recipients of the personal data; (ii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (iii) the existence of the right of access to and the right to rectify the personal data; and (iv) whether the personal data will be used for direct marketing purposes.

Where personal data has been obtained from a party other than the *data subject*, the *data controller* must at the time of processing the personal data or if a disclosure to a third party is envisaged, provide *data subjects* with the *fair processing information* detailed above.

Rights to access information

Data subjects have the right to request their *subject access information* by a request to the *data controller*.

Objection to direct marketing

A *data subject* has the right to be informed before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing. A *data subject* must also be expressly given the right to object to such disclosures or uses.

Other rights

Data subjects may request the rectification, erasure or blocking of personal data where the processing does not comply with the provisions of the Data Protection Law.

A *data subject* has the right to object at any time on reasonable grounds relating to his particular situation to the processing of personal data relating to him. Where there is a justified objection, the relevant personal data must be removed from the processing operation that was being conducted by the *data controller*.

Security

Security requirements in order to protect personal data

The Data Protection Law refers to the *general data security obligations* and other general security obligations.

Specific rules governing processing by third party agents (processors)

The Data Protection Law states that the *data controller* must, where processing is carried out on its behalf, choose a *data processor* which provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and must ensure compliance with those measures. There is no obligation to have a written contract with such *data processors*.

Notice of breach laws

In the event of an unauthorised intrusion, either physical, electronic or otherwise, to any personal data database, the *data controller* or the *data processor* carrying out the *data controller's* function at the time of the intrusion must inform the Commissioner of the incident as soon as reasonably practicable. There is no obligation to notify the *data subjects*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The Law contains restrictions on *transborder dataflows*. *Transborder dataflows* may take place where there is an adequate level of protection for the personal data, ensured by the laws and regulations applicable to the recipient. For this purpose, a jurisdiction has an adequate level of protection where that jurisdiction is listed as an acceptable jurisdiction under the Regulations or with the written approval of the Commissioner. A list of "adequate" data protection regimes is available at http://difc.ae/adequate-data-protection-regimes.

Where there is an inadequate level of protection, *transborder dataflows* may only occur where: (i) the *data subject* has given his written approval to the proposed transfer; (ii) the transfer is necessary for the performance of a contract with the *data subject* or in the interests of the *data subject*; (iii) the transfer is necessary or legally required on grounds important in the interests of the DIFC, or for the establishment, exercise or defence of legal claims; (iv) the transfer is necessary in order to protect the vital interests of the *data subject*; (v) the transfer is made from a public register; (vi) the transfer is necessary for compliance with any legal obligation to which the *data controller* is subject or the transfer is made at the request of a regulator, the police or an other government agency; (v) the transfer is necessary to uphold the legitimate interests of the *data controller* recognised in the international financial markets except where such interests are overridden by legitimate interests of the *data subject*; or (vi) the transfer is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or obligations relating to prevention or detection of any crime that apply to a *data controller*.

A transfer may also take place where the Commissioner has authorised the transfer and the *data controller* applies adequate safeguards with respect to the protection of personal data.

Notification and approval of national regulator (including notification of use of Model Contracts)

A *data controller* must notify the Commissioner where any personal data processing operations involve the transfer of personal data to a recipient outside the DIFC which is not subject to laws and regulations which ensure an adequate level of protection.

Use of binding corporate rules

No.

Enforcement

Sanctions

The Commissioner has the power to issue directions preventing the processing of personal data. Where such directions are not complied with, the *data controller* may be subject to a fine of USD 15,000 and is liable for payment of compensation.

Fines can also be levied in other circumstances. The current schedule of fines issued by the DIFC Authority lists the maximum fine as USD 25,000 for failure to register with the Commissioner. Other fines include USD 20,000 for transferring personal data outside the DIFC without obtaining a required permit and USD 10,000 for processing sensitive personal data without obtaining a required permit.

Practice

We are not aware of any enforcement actions over the last 12 months.

Enforcement authority

The Commissioner has the power to issue directions in respect of any contravention of the Data Protection Law and the Regulations. The DIFC Court has jurisdiction to hear appeals against decisions made by the Commissioner.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

None specifically relevant to ePrivacy issues.

Cookies

Conditions for use of cookies

None specifically relevant to cookies.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The Data Protection Law does not specifically set out rules in relation to the use of electronic direct marketing. However, in accordance with certain general provisions of the Data Protection Law, the *data subject* has the right to be informed before their personal data is used on their behalf and may object to the disclosure or use of their personal data for direct marketing purposes.

Conditions for direct marketing by e-mail to corporate subscribers

The provisions of the Data Protection Law in respect of direct marketing only apply to natural persons.

Exemptions and other issues

Not applicable.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The Data Protection Law does not specifically set out rules in relation to direct marketing by telephone. However, in accordance with certain general provisions of the Data Protection Law, the *data subject* has the right to be informed

before their personal data is used on their behalf and may object to the disclosure or use of their personal data for direct marketing purposes.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The provisions of the Data Protection Law in respect of direct marketing only apply to natural persons.

Exemptions and other issues

Not applicable.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The Data Protection Law does not specifically set out rules in relation to direct marketing by fax. However, in accordance with certain general provisions of the Data Protection Law, the *data subject* has the right to be informed before their personal data is used on their behalf and may object to the disclosure or use of their personal data for direct marketing purposes.

Conditions for direct marketing by fax to corporate subscribers

The provisions of the Data Protection Law in respect of direct marketing only apply to natural persons.

Exemptions and other issues

Not applicable.

Estonia.

Contributed by Raidla Lejins & Norcous

General | Data Protection Laws

National Legislation

General data protection laws

The Personal Data Protection Act (Isikuandmete kaitse seadus) (the "**DPA**") dated 15 February 2007 implemented the *Data Protection Directive*.

Entry into force

The DPA entered into force on 1 January 2008.

National Regulatory Authority

Details of the competent national regulatory authority

Data Protection Inspectorate (the "**Inspectorate**")
Väike-Ameerika 19
10129 Tallinn
Estonia

www.aki.ee

Notification or registration scheme and timing

Data controllers are required to register the processing of sensitive personal data with the Inspectorate at least one month prior to commencing processing. The Inspectorate will refuse to register the processing of sensitive personal data if: (i) there is no legal basis for such processing; (ii) the conditions of processing do not comply with the requirements of the DPA; or (iii) the security measures applied do not ensure compliance with the requirements of the DPA. Registration with the DPA does not require the payment of any fees.

Exemptions

Processing of personal data other than sensitive personal data does not have to be registered with the Inspectorate.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer. However, if one is appointed, the processing of sensitive personal data does not have to be registered with the Inspectorate.

Personal Data

What is personal data?

According to the DPA personal data means any information relating to an identified and identifiable natural person irrespective of the form or format of the data. Therefore, the definition of personal data in the DPA is closely based on the *standard definition of personal data*.

Is information about legal entities personal data?

No. The DPA does not apply to information about legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met.

Are there any formalities to obtain consent to process personal data?

Consent is valid only if it is based on the free will of the *data subject*. Silence or inactivity shall not be deemed as a valid consent. Consent may be partial and conditional.

Consent must also be specific and so to obtain it the *data controller* must specify the: (i) data for which consent is given; (ii) purposes of processing the data, (iii) parties to whom the data may be transferred; (iv) conditions for transferring the data to third parties; and (v) rights of the *data subject* concerning further processing of his or her personal data. It is also necessary to notify the *data subject* of the contact details of the relevant *data controller* and *data processor(s).*

Consent shall be given in a format which can be reproduced in writing (for example, by e-mail, online via a website, signed document, or fax) unless adherence to such a formality is not possible due to the specific manner of the data processing. If the consent is given together with another declaration of intent, the consent must be clearly distinguishable.

In case of a dispute, it is presumed that the *data subject* has not provided consent. The burden of proof regarding the provision of consent is on the *data controller*.

There are no further formalities to obtain consent to process personal data of employees.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data include the following: (i) the *standard types of sensitive personal data*; (ii) data regarding genetic information; (iii) biometrical data (such as data regarding fingerprints, handprints, eye irises and genetic data); and (iv) information about committed criminal offences (or being a victim of these) prior to a public court hearing.

Are there additional rules for processing sensitive personal data?

As indicated above, processing of sensitive personal data is subject to registration with the Inspectorate. The exemptions provided in Article 8 (2) of the *Data Protection Directive* are not fully transposed into the DPA. However in practice these exemptions are relied upon extensively.

Are there any formalities to obtain consent to process sensitive personal data?

Some additional formalities are required to obtain consent to process sensitive personal data. First, such consent must be in a format which can be reproduced in writing (no exceptions apply), and secondly, such a consent must clearly state that the data to be processed are sensitive personal data.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

All persons engaged in the processing of personal data (i.e. both *data controllers* and *data processors*) are responsible for compliance with the DPA, except natural persons processing personal data for personal purposes.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to personal data, as stipulated above, irrespective of the form or nature in which the data are recorded or stored.

Rights of Data Subjects

Compensation

The DPA itself does not contain any specific provisions regarding *data subject's* right to claim compensation for damages caused by violations of the DPA. However, the DPA stipulates that the *data subject* may claim compensation for damages pursuant to general laws regarding such claims – the Law of Obligations Act (Võlaõigusseadus) and State Liability Act (Riigivastutuse seadus).

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. This is not required if: (i) the *data subject* has given his consent for the processing of personal data; (ii) the *data subject* is aware of the scope, sources and contact details of the *data controller* in case the *data subject* is not the source of the personal data; (iii) the processing of personal data is carried out pursuant to legal acts; (iv) the provision of the *fair processing information* is impossible; or (v) the provision of the *fair processing information* would have harmful consequences as stipulated in the DPA. The DPA does not stipulate an obligation to provide this information in Estonian. However, if reasonably possible, this information should be provided in a language understandable to the *data subject*.

Rights to access information

Data subjects may obtain their *subject access information* by a request to *data controllers*. The data shall have to be submitted in a format requested by the *data subject*, if possible. When submitting information on paper, the *data controller* may request a fee up to EUR 0.19 per every submitted page (starting from the 21st page).

Objection to direct marketing

Under the DPA, if the processing of personal data is not explicitly permitted according to the law, the *data subject* may at any time request: (i) the termination of processing of personal data; (ii) the termination of publishing or granting access to personal data; and/or (iii) the deletion or closing of gathered personal data.

Other rights

Data subjects have the right to request rectification of inaccurate personal data.

Security

Security requirements in order to protect personal data

Data controllers must fulfil the *general data security obligations*. Additionally, *data controllers* have an obligation to keep records of devices and software under their control which are used for the processing of personal data, by recording the following data: (i) name, type, location and manufacturer of the devices; and (ii) name and version of the software and name and contact details of its manufacturer.

Specific rules governing processing by third party agents (processors)

Data processors are obliged to fulfil *standard processor obligations*. Additionally, *data controllers* are obliged to ensure that *data processors* who are processing personal data under their supervision have received training regarding data protection.

Notice of breach laws

The DPA does not contain any obligation to inform the Inspectorate or *data subjects* of a security breach.

Specific notice of breach requirements apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive* and have been implemented into national law in the Electronic Communications Act (the "**ECA**").

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

As a general rule, personal data may only be transferred to countries which have adequate levels of data protection (this includes transfers to whitelisted countries). Transferring personal data to countries which do not have adequate levels of data protection is permitted only with the Inspectorate's approval if: (i) the *data controller* guarantees that the *data subject's* rights in such country will not be violated (for example, by using the *Model Contracts*); or (ii) if, considering the circumstances, for this specific case the level of data protection in such country is adequate.

Data may also be transferred to countries which do not have adequate levels of data protection without the Inspectorate's approval if: (i) the *data subject* has provided his/her consent for this; (ii) the data are being transferred for the protection of the *data subject's* life, health and freedom if it is impossible to acquire the *data subject's* consent; or (iii) a third party requests information which has been received or created in the course of performance of public duties pursuant to the law and additional access limitations have not been stipulated for it.

Notification and approval of national regulator (including notification of use of Model Contracts)

Approval for a transborder dataflow is required in certain circumstances (see above). There is no separate notification obligation regarding the use of *Model Contracts*, as these are submitted to the Inspectorate in connection with applying for the approval of a transborder dataflow.

Use of binding corporate rules

Estonia is part of the mutual recognition club for *binding corporate rules*. However, the Inspectorate has not issued any public opinions on the use of binding corporate rule and these are not yet commonly used in practice.

Enforcement

Sanctions

Violations of the requirements for the processing of personal data stipulated in the DPA are treated as misdemeanours and are punishable by a fine of up to EUR 32,000. In addition, the Penal Code stipulates a criminal offence of illegally disclosing, enabling access to or transferring sensitive personal data, either: (i) for personal gain; or (ii) if significant damage is caused to the rights or interests of another person that are protected by law. This offence is punishable by a pecuniary punishment or up to one year's imprisonment.

Practice

Pursuant to the information available on the Inspectorate's website, the Inspectorate issued 115 precepts in 2011. Penalty payments and fines were applied on 38 occasions. There were also 34 misdemeanour proceedings concluded. There were 818 challenges and complaints issued to the Inspectorate (this number has grown steadily over the last few years, from just 110 in 2007).

In relation to the highest penalty levied to date, the Inspectorate does not have any statistics on this matter. However, the imposition of penalty payments and fines is rather rare (although it is becoming more widespread) and in practice the

Inspectorate usually only takes such measures if a *data controller* violates the law and does not bring its activities into compliance even after a precept or a warning has been issued by the Inspectorate.

Enforcement authority

Enforcement measures can be taken both by the Inspectorate (which is authorised to apply administrative coercion, initiate misdemeanour proceedings and, if necessary, impose punishments) and the courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The ECA transposed Article 13 of the *Privacy and Electronic Communications Directive* into Estonian law. However, some aspects of the marketing methods detailed below are regulated by the Information Society Services Act (Infoühiskonna teenuse seadus) and the Law of Obligations Act (Võlaõigusseadus).

In July 2010, amendments to the ECA and the Information Society Services Act entered into force which transferred most of the regulation regarding direct marketing into ECA and addressed the principal shortcomings of the old rules. Under the new rules, direct marketing is regulated where it involves the use of "electronic contact data" for direct marketing purposes. Electronic contact data is defined as data which enables transmission of information to a person via an electronic network, such as fax, e-mail, SMS or MMS.

The ECA was amended on 22 February 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Currently, it is only necessary to inform users of the use of cookies and offer them the right to refuse their use. This requirement arises indirectly from a general data protection provision of the ECA included therein already since adoption of the ECA in 2004 and is not the result of implementation of the cookie provision as provided by the *Privacy and Electronic Communications Directive* and amended by the *Citizens' Rights Directive*. At the moment there are no public plans to adopt any additional regulation to implement the cookie provision.

Regulatory guidance on the use of cookies

There is no regulatory guidance on the use of cookies. Furthermore, although the Inspectorate has published numerous data protection related guidelines and written opinions on their website, none of these discuss the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Pursuant to the ECA, the use of electronic contact data for the purpose of direct marketing to a user (who is a natural person) via an electronic communications service is allowed only if the person has given his prior consent. Such consent is subject to the same requirements as stipulated for the general data processing consent in the DPA. Under ECA, the burden of proof relating to provision of consent is placed upon the person on behalf of whom the direct marketing is performed.

Conditions for direct marketing by e-mail to corporate subscribers

The ECA does not require consent for the use of electronic contact data for the purpose of direct marketing to a user (who is a legal person) via an electronic communications service.

Exemptions and other issues

It is permitted to send an e-mail for the purposes of direct marketing if the *similar products and services exemption* applies (save that the right to object must be available using an electronic communications network). For this exemption to apply the recipient's details only need to have been collected in connection with the sale on negotiation for sale of products and services. There is no need for an actual contract to have been formed.

Direct marketing e-mails are also prohibited if: (i) the identity of the sender is disguised or concealed; or (ii) an electronic opt-out address is not provided. Certain additional restrictions apply depending on the contents of the email (e.g. if the email relates to lotteries or promotional offers).

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The direct marketing rules in the ECA do not apply to multi-party telephone calls taking place in real-time. Such direct marketing is regulated by the Law of Obligations Act. Communicating offers directly to an individual subscriber by telephone is permitted unless the individual subscriber has expressly forbidden such communication.

Direct marketing to a telephone answering machine of individual subscribers falls under the scope of the ECA and is allowed on the same conditions as direct marketing by e-mail to individual subscribers, described above.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Estonian law does not expressly regulate direct marketing by multi-party real-time telephone calls to corporate subscribers. Therefore, the restrictions above do not apply in the case of direct marketing to corporate subscribers in such a manner.

Direct marketing to a telephone answering machine of corporate subscribers falls under the scope of the ECA and is allowed on the same conditions as direct marketing by e-mail to corporate subscribers, described above.

Exemptions and other issues

None.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax is subject to the same rules as direct marketing by emails (see above).

Conditions for direct marketing by fax to corporate subscribers

Direct marketing by fax is subject to the same rules as direct marketing by emails (see above).

Exemptions and other issues

Direct marketing by fax is subject to the same rules as direct marketing by emails (see above).

Finland.

Contributed by Hannes Snellman Attorneys Ltd

General | Data Protection Laws

National Legislation

General data protection laws

The Finnish Personal Data Act (Henkilötietolaki 1999/523) (the "**DPA**") dated 22 April 1999 implemented the *Data Protection Directive*.

Entry into force

The DPA came into force on 1 June 1999.

National Regulatory Authority

Details of the competent national regulatory authority

The Office of the Data Protection Ombudsman (supervises the processing of personal data in order to achieve the objectives of the DPA) (the "**Ombudsman**")
P.O. Box 315
00181 Helsinki
Finland

www.tietosuoja.fi

The Data Protection Board/Ministry of Justice (deals with questions of principle relating to the processing of personal data) (the "**Board**")
P.O. Box 25
00023 Council of State
Finland

www.om.fi

Notification or registration scheme and timing

Unless the processing is exempt, the *data controller* must notify the Ombudsman of automated data processing and any transfer of data outside of the EEA that requires such a notification no later than 30 days before processing commences. No approval is required and no official fee is payable for the making of the notification.

Besides the notification requirement, the *data controller* must draw up a description of each personal data file, in which the purpose and main principles of data processing are explained. The description of the data file must be kept available for review for all *data subjects*.

Exemptions

Every *data controller* who is processing personal data must notify the Ombudsman unless they are exempt. Exemptions apply if, inter alia: (i) the *data subject* has unambiguously consented to the processing; (ii) the *data subject* has given an assignment for processing, or the processing is necessary in order to perform a contract to which the *data subject* is a party or in order to take steps at the request of the *data subject* before entering into a contract; (iii) processing is necessary, in an individual case, in order to protect the vital interests of the *data subject*; (iv) processing is based on a law; (v) there is a relevant connection between the *data subject* and the operations of the *data controller*, based on the *data subject* being a client or member of, or in the service of, the *data controller*; (vi) the data relates to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within that grouping; or (vii) the Board has granted permission for the processing. In addition, derogation may be provided by a decree if it is evident that the processing of personal data does not compromise the protection of the privacy of the *data subject*, or his rights of freedom.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer. However, the description of each data file must include information on the person responsible for the processing of personal data in order for the *data subjects* to exercise their rights under the DPA.

Personal Data

What is personal data?

The DPA defines personal data as any information on a private individual and any information on his or her personal characteristics or personal circumstances, where these are identifiable as concerning him or her or the members of his or

her family or household. This definition is to be interpreted in a way that all information concerning a private individual, e.g. name, address, phone number, e-mail address, is to be understood as personal data. The definition of personal data in the DPA is therefore closely based on the *standard definition of personal data*.

The requirement that personal data "relate to" an individual was considered by the Board in the case of TTVK (Dno. 2/936/2005). The Board stated that an IP address can be regarded as personal data. Although an IP address alone does not identify a person, it can be used together with other means in order to identify a person.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the general prerequisites for processing are met. The prerequisites, to a great extent, conform with *standard conditions for processing personal data*.

A *data controller's* processing of personal data must be appropriate and justified. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of the personal data intended to be recorded in the file or its organisation into a personal data file.

The DPA contains exemptions for certain types of processing. Processing for special purposes (e.g. research and statistics) is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

No. According to the DPA, consent means any voluntary, detailed and conscious expression of will whereby the *data subject* approves the processing of his/her personal data. It is, however, advisable to obtain written consent because the *data controller* has the burden of proof concerning the obtained consent. The DPA also provides that any consent given by the *data subject* can be withdrawn at any time.

Sensitive Personal Data

What is sensitive personal data?

Personal data is deemed to be sensitive if it relates to or is intended to relate to: (i) the *standard types of sensitive personal data*; (ii) a criminal act, punishment or other criminal sanction; or (iii) the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person.

In addition, the DPA contains limitations as to the processing of personal identity numbers (these are not sensitive personal data as such). According to the guidance of the Ombudsman, the use of biometric recognition or processing of biometric information should be based on special legislation or the consent of the *data subject*.

Are there additional rules for processing sensitive personal data?

The processing of sensitive data is prohibited. Sensitive data may only be processed under specific conditions described in the DPA. The conditions are in close conformity with the *standard conditions for processing sensitive personal data*.

The Board may grant permission for the processing of sensitive data for a reason pertaining to an important public interest. The permission may be granted for a fixed period or for the time being; it shall contain the rules necessary for the protection of the privacy of the *data subject*.

It should also be noted that, according to the Act on the Protection of Privacy in Working Life, which lays down provisions on the processing of personal data about employees, the employer only has the right to process information concerning the employees' state of health if the information has been collected from the employees themselves, or elsewhere with the employees' written consent, and the information needs to be processed in order: (i) to pay sick pay or other comparable health-related benefits; (ii) to establish whether there is a justifiable reason for absence; or (iii) to assess the employees' working capacity on the basis of information concerning his/her state of health, in accordance with their express wishes.

Are there any formalities to obtain consent to process sensitive personal data?

There are no formalities to obtain consent to process sensitive personal data. Thus, the position is the same as for other personal data (see above). However, it is highly advisable to obtain consent in a written format, despite the DPA being silent on this matter.

A consent given by an employee or prospective employee to the processing of his/her sensitive personal data contained in his/her criminal records has, in legal praxis by the Ombudsman, been considered as given involuntarily. The consent to the processing of such sensitive personal data would thus not be effective and the processing of sensitive personal data would be in breach of the provisions of the DPA.

Finland.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The responsibility for compliance with the DPA lies with the *data controller*. *Data processors* are not subject to the DPA. The provisions of the DPA apply to the processing of personal data.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to: (i) the automatic processing of personal data; and (ii) the processing of personal data where the data constitute a personal data file or a part thereof. A personal data file is defined in the DPA as a set of personal data, connected by a common use and processed fully or partially automatically or sorted into a card index, directory or other accessible form so that the data pertaining to a given person can be retrieved easily and at reasonable cost.

Rights of Data Subjects

Compensation

The *data controller* is liable to pay compensation for economic and other loss suffered by the *data subject* or another person as a result of the processing of personal data in violation of the DPA. The provisions of the Tort Liability Act (412/1974) shall apply to the applicable liability in damages. However, the *data controller's* liability to pay damages is not dependent on its default or negligent act. Thus, the liability for damages is a strict liability as defined in the Tort Liability Act. In order to claim damages the *data subject* or another person must prove the damage suffered and the action for damages must be brought in a district court.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. The *data subject* must also be informed of the regular destinations of disclosed data and how the *data subject* may exercise his rights with respect to the processing in question. In practice, the obligation to provide information is satisfied by including the information in the description of the data file. There is no obligation to provide this information in a local language (i.e. Finnish or Swedish). Thus, the information may be provided in English, for example.

The duty of providing the *fair processing information* may be derogated from: (i) if the *data subject* already has the relevant information; (ii) if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances; or (iii) where the data is collected from elsewhere than the *data subject*, if the provision of the information to the *data subject* is impossible or unreasonably difficult, or if it significantly damages or inconveniences the *data subject* or the purpose of the processing of the data and the data is not used when making decisions relating to the *data subject*, or if there are specific provisions in an Act on the collection, recording or disclosure of the data.

Additionally, certain specific rules apply with regard to the provision of information to the *data subject* on the processing of data contained in a credit data file and the related right of access.

Rights to access information

Data subjects may obtain their *subject access information* upon a signed request or otherwise comparably verified document or personal appearance at the premises of the *data controller*. The *data controller* may charge for the provision of access to the data only if less than one year has passed since the previous instance of providing the *data subject* with access to data in the file. The charge shall be reasonable and it shall not exceed the immediate costs of providing access to the data.

Objection to direct marketing

A *data subject* has the right to prohibit the *data controller* from processing personal data for direct advertising, distance selling, other direct marketing, market research, opinion polls, public registers or genealogical research. No time is specified by which direct marketing must cease.

Other rights

At the request of the *data subject*, or on his own initiative, the *data controller* must, without undue delay, rectify, erase or supplement personal data contained in his personal data file which is erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing.

The making of a decision on the basis of certain characteristics of a *data subject*, where involving solely automatic data processing and having legal consequences to the *data subject*, is permitted only if certain criteria are met.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations*.

Specific rules governing processing by third party agents (processors)

The *data processor* must, before starting to process the data, provide the *data controller* with appropriate commitments and other adequate guarantees of the security of the data as provided above. It is recommended to stipulate commitments and guarantees in a contract between the *data controller* and *data processor*. Anyone who has gained knowledge of the characteristics, personal circumstances or economic situation of another person while carrying out measures relating to data processing must not disclose the data to a third person in contravention of the DPA.

Notice of breach laws

The DPA does not contain any obligation to inform the Ombudsman or *data subjects* of a security breach.

Specific notice of breach laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. The amendments were implemented into the ECA (as defined later).

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the *data controller* satisfies the *standard conditions for transborder dataflow*. Alternatively, the personal data may be transferred to countries outside of the EEA if: (i) the country in question guarantees an adequate level of data protection; or (ii) a modified version of the *Model Contracts* is used.

Notification and approval of national regulator (including notification of use of Model Contracts)

No approval of transfer is required. However, the Ombudsman must be notified when a data transfer contract used does not follow the *Model Contracts*. The Ombudsman need not be notified when unmodified *Model Contracts* are used. The *data controller* shall also notify the Ombudsman of the transfer of personal data to outside the European Union or the EEA, if a transfer is made on the basis of the *data controller's* own assessment of adequacy of protection in the country in question or if: (i) the transfer is made from a file from which the disclosure of data, either generally or for special reasons, has been specifically provided in an Act; or (ii) the *data controller*, by means of contractual terms or otherwise, has given adequate guarantees of the protection of the privacy and the rights of individuals, and the Commission has not found the guarantees inadequate.

Use of binding corporate rules

The use of *binding corporate rules* to affect intra-group transfers is enabled, provided that all group companies accept such rules as binding and that the rules are approved by the data protection authorities prior to transfers of personal data. The Ombudsman has not yet acted as a leading authority in processes regarding the approval of *binding corporate rules*, but has approved *binding corporate rules* where the application for such rules was made to, and approved by, another supervisory authority in Europe, for example, Atmel, GE.

Enforcement

Sanctions

There are financial penalties for a personal data violation under the DPA. The penalties for a personal data offence, for breaking into a personal data file and for violation of the secrecy obligation are provided for in the Finnish Penal Code (39/1889). The penalties range from a fine to one year in prison.

The *data controller* is liable to compensate for economic and other loss suffered by the *data subject* or another person as a result of the processing of personal data in violation of the DPA.

Practice

In 2011, the number of requests for guidance made to the Ombudsman by *data controllers* was 528 (compared to 414 in 2010). The number of requests for investigation or guidance made by *data subjects* was 957 (compared to approximately 900 in 2010).

In addition, in 2011 the Ombudsman gave 64 (compared to 84 in 2010) statements to the public prosecutors before any prosecution. There were 17 decisions made by the Board in 2011 (compared to 6 decisions in 2010).

There is currently no statistical data on the level of penalties imposed in 2008-2011.

Enforcement authority

The Ombudsman promotes good processing practice and issues directions and guidelines so as to ensure unlawful conduct against the DPA is not continued or repeated. Where necessary, the Ombudsman shall refer the matter to be dealt with by the Board or report the matter for prosecution. In addition, the Ombudsman shall decide matters brought to the Ombudsman's attention by *data subjects* by ordering *data controllers* to grant rights of access to the *data subject* or to rectify an error.

The Board deals with questions of principle relating to the processing of personal data where these are significant to the application of the DPA, as well as making decisions in matters of data protection.

The decisions of the Ombudsman and the Board are subject to appeal in accordance with the provisions of the Finnish Administrative Judicial Procedure Act (586/1996). The Ombudsman and the Board may only impose the threat of a fine in certain data protection-related matters.

Prosecutions for criminal offences are brought before the Finnish District Courts and may lead to fines or imprisonment. Claims for damages by *data subjects* are also brought before the Finnish District Courts as independent claims or integrated with criminal proceedings. The public prosecutor shall hear the Ombudsman prior to bringing charges for an action violating the DPA. When hearing a case of this sort, the Court shall reserve the Ombudsman an opportunity to be heard.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Finnish Act on the Protection of Privacy in Electronic Communications (Sähköisen viestinnän tietosuojalaki 2004/516) (the "**ECA**") dated 16 June 2004 implemented Article 13 of the *Privacy and Electronic Communications Directive*. The ECA came into force on 1 September 2004.

The ECA was amended on 8 April 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

As a consequence of the implementation of the *Citizens' Rights Directive*, consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. Although the ECA does not expressly refer to the use of browser settings as a means to obtain consent, such means have, however, been mentioned as such in the draft documents of the legislation. There is no express requirement for consent to be "prior" to the use of a cookie, but it seems clear, in the light of the draft documentation of the legislation, that consent will need to be obtained beforehand.

Regulatory guidance on the use of cookies

There is currently no regulatory guidance on the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under the ECA, it is not permitted to send unsolicited direct marketing to individuals by electronic communication, such as e-mail, without the person's prior consent.

Conditions for direct marketing by e-mail to corporate subscribers

Under the ECA, direct marketing by electronic communication to legal persons is allowed if the recipient has not specifically refused it. According to the guidance note of the Ombudsman, although a personal e-mail address based on a company's domain name (e.g. individual@company) can be used for direct marketing purposes, the recipient is regarded as an individual and a prior consent is required, unless the direct marketing has been sent to that person based on his job description.

Exemptions and other issues

The ECA allows the *similar products and services exemption*. According to the interpretation of the Ombudsman, in order to send direct marketing to an individual without the person's prior consent, marketing may be performed only by using the same electronic means (e.g. text messages, e-mail) through which a service or a product has been bought or obtained.

The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out email address is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing by telephone to individual subscribers, when performed by an individual, is not permitted if the recipient has specifically requested not to receive such marketing.

The opportunity to opt out must be reserved in each occurrence of direct marketing easily and at no separate cost. Therefore, the individual subscriber must be able to refuse use of his personal data for direct marketing purposes during each call. In addition, the DPA requires that the individual performing the direct marketing must be able to provide the subscriber with information on the data register and *data controller* (including address) from whom the personal data has been acquired when requested. The individual subscriber is also entitled to inform the original *data controller* of his request not to receive direct marketing by telephone.

Direct marketing by telephone must be identified as marketing and the identity of the party on whose behalf the marketing is conducted must be provided.

If the individual subscriber has under the DPA prohibited use of his personal data for purposes of direct marketing, his personal data may not be utilised for direct marketing at all.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Direct marketing by telephone to corporate subscribers is not permitted if the recipient has specifically requested not to receive such marketing. The opportunity to opt-out must be reserved in each occurrence of direct marketing, easily and at no separate cost.

If the personal data of the employee of the corporate subscriber is used in telephone marketing, the individual performing the direct marketing must be able to provide the employee with information on the data register and *data controller* (including address) from whom his personal data have been acquired when requested.

Direct marketing by telephone must be identified as marketing and the identity of the party on whose behalf the marketing is conducted must be provided.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Under the ECA, it is not permitted to send unsolicited direct marketing to individuals by electronic communications, such as fax, without the person's prior consent.

The ECA prohibits the practice of sending a fax for direct marketing purposes that disguises or conceals the identity of the sender and lacks a valid address to which the recipient may send a request for termination of communications. The ECA also requires that each electronic direct marketing message must, upon receipt, be unmistakably identifiable as a marketing message.

Conditions for direct marketing by fax to corporate subscribers

Under the ECA, direct marketing by electronic communication to legal persons is not permitted if the recipient has specifically requested not to receive such marketing. The opportunity to opt out must be reserved for any legal person in each occurrence of direct marketing easily and at no separate cost and the party undertaking direct marketing must give clear notification of the possibility of such refusal.

The ECA prohibits the practice of sending a fax for direct marketing purposes that disguises or conceals the identity of the sender and lacks a valid address to which the recipient may send a request for termination of communications. The ECA also requires that each electronic direct marketing message must, upon receipt, be unmistakably identifiable as a marketing message.

Exemptions and other issues

No exemptions apply.

France.

General | Data Protection Laws

National Legislation

General data protection laws

The *Data Protection Directive* has been implemented in the French Data Protection Act of 6 January 1978 (the "**DPA**"). The DPA has been modified twice in 2011. Firstly by the Law no. 2011-334 of 29 March 2011 and secondly by the Ordinance no. 2011-1012 of 24 August 2011 (the "**Ordinance**").

Entry into force

The DPA, as amended to implement the *Data Protection Directive*, came into force on 6 August 2004.

National Regulatory Authority

Details of the competent national regulatory authorities

Commission Nationale de l'Informatique et des Libertés (the "**CNIL**")

8, rue Vivienne
CS 30223
75083 Paris
Cedex 02
France

www.cnil.fr

Notification or registration scheme and timing

The usual regime for the processing of personal data is that of a prior declaration to the CNIL.

However, the DPA also provides for a limited number of cases where express authorisation must be obtained from the CNIL. The cases where an express authorisation is needed under the DPA include, among others: (i) the processing of certain categories of sensitive data; (ii) the transfer of data outside the EEA to a country without adequate protection; (iii) automated processing which consists of a selection of people and is aimed at excluding some of them from the advantages of a right, a benefit or a contract; (iv) automated interconnection files; and (v) biometric identity checks, for instance, for access controls. The processing of data relating to criminal offences and proceedings, health or social security numbers is also restricted.

In all cases where a declaration or an authorisation is required, the *data controller* has to complete a form available on the CNIL's website. For common types of processing (e.g. payroll, management of employees, customer files) simplified forms can be used. Forms can be submitted electronically. There is no charge to make a declaration or request an authorisation.

If express authorisation is required, processing can only commence once that authorisation is given. If the CNIL fails to respond within two months of the notification (this period can be extended by two months by the CNIL's President), it will be deemed to have refused that authorisation. If express authorisation is not required, processing can start from the date the *data controller* receives a receipt from the CNIL for its declaration.

In 2011, 84,243 declarations were filed with the CNIL.

Exemptions

Every *data controller* who is processing personal data must notify the CNIL, unless exempted. Exemptions apply in respect of: (i) maintenance of a public register; (ii) certain processing relating to non-profit-making organisations; (iii) accounts and records of the *data controller*; (iv) processing for which the *data controller* has appointed a personal data protection officer responsible for ensuring the application of the obligations provided by the DPA and for keeping a register of processing (except where processes are involved that require an authorisation or an opinion and this includes, in general, processes where a transborder dataflow is contemplated); and (v) other processing exempt by a specific decision of the CNIL.

Appointment of a data protection officer

The DPA permits organisations to appoint data protection officers on an optional basis and this can provide an exemption from notification. According to the CNIL2011 activity report, 8,635 *data controllers* have appointed a data protection officer.

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. The CNIL has a very broad conception of personal data.

There have been a number of court decisions about the concept of personal data. For example, the Paris Court of Appeal has decided that an IP address does not qualify as personal data and that, consequently, the processing of IP addresses and related users' names obtained from/communicated by internet service providers without prior notification to the CNIL constituted admissible evidence of illicit exchange of music files (see CA Paris, 13ème ch., 27 April 2007 no. 338935).

However, the CNIL considers that these decisions do not reflect the *Opinion on Personal Data* and the broad definition of personal data as set out in Article 2 of the DPA. Therefore, the CNIL has asked the Minister of Justice to lodge an appeal against these decisions before the Supreme Court (Cour de Cassation) and suggested that an interlocutory question on the nature of IP addresses be submitted to the European Court of Justice. No clear decision has yet been taken by the Supreme Court on IP addresses. However, in two recent decisions, the criminal chamber of the Supreme Court decided that investigations on the internet by a sworn agent, acting on behalf of a society for producers and publishers of musical and audio-visual recordings collecting IP addresses to detect illegal activities, but not using any automatic search processes, did not amount to data processing relating to offences that would require a prior authorisation by the CNIL. (see Cass. crim., 13 January 2009, no. 08-84.088; Bull. crim. 2009, no. 13; and Cass. crim., 16 June 2009, no. 08-88560; Juris-Data no.2009-049199). The Constitutional Council, in its decision of 10 June 2009 (no. 2009-5890) on the Hadopi law, decided that collecting data enabling the identification of the owner of a connection to the internet is a processing of personal data. This decision has indirectly qualified IP addresses as personal data.

Please note that the CNIL does not distinguish between a static and dynamic IP address and considers that both qualify as personal data.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities. It may therefore also apply to any individual acting as a sole trader or as a member of a partnership.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met.

The DPA contains exemptions for certain types of processing (for instance for public security or state security).

Are there any formalities to obtain consent to process personal data?

In theory, except in specific cases where express consent is required by law, consent can be express, written, oral or implied. However, in practice, a *data subject's* consent must be in French and given either in writing or by a click-through, if given over the internet. Obtaining consent from employees is deemed impossible, except in limited cases, as it is considered that it will never be given freely by the employee.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes the *standard types of sensitive personal data*. Some guidance has been given on the concept of sensitive data. For example, a court decision has ruled, before the implementation of the *Data Protection Directive* into French law, that a photograph of a naked person uploaded on the internet qualifies as sensitive data as it indirectly revealed such person's sex life (see TGI Privas, 3 September 1997, JCP E 1999, no. 21, p. 913).

The DPA does not treat information about offences, convictions or security measures as sensitive personal data but does place very strict controls over its processing by requiring a prior authorisation.

Are there additional rules for processing sensitive personal data?

The processing of sensitive data is prohibited under the DPA, unless processed with the consent of the *data subject* or the *standard conditions for processing sensitive personal data* are met (however, please note these conditions do not include processing pursuant to a legal obligation imposed in an employment context). The DPA also provides a limited number of additional processing conditions where sensitive personal data is processed for statistical medical research purposes or if the processing is in the public interest and authorised by the CNIL. In some cases, a specific authorisation from the CNIL is required to process such categories of data.

Despite not being classed as sensitive personal data, the processing of information about offences has to be authorised by the CNIL (unless the *data controller* is a representative of justice (auxiliaires de justice)). There is a simplified authorisation procedure for offences recorded by merchants on a point of sale. In addition, there are particular procedural rules regarding data processing implemented on behalf of the French State for the purpose of the prevention, investigation, or proof of criminal offences; the prosecution of offenders; or the execution of criminal sentences or security measures.

Processing of biometric data is subject to prior authorisation of the CNIL and *data subjects* have to be fully informed of such processing. The authorisation process is simplified in certain cases of standard processing, for example, access control. Fingerprints may generally only be registered on a stand alone medium, such as a USB key, but not on a centralised database. In 2011, the CNIL authorised biometric identification using both fingerprints and networks of veins in the hand for the first time.

Transfer of sensitive data to countries outside the EEA is not prohibited but has to be clearly justified, since the CNIL deems local processing is more appropriate for this type of personal data.

Are there any formalities to obtain consent to process sensitive personal data?

The position is the same as for the processing of personal data (see above) except that the DPA specifies that consent must be explicit.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. *Data processors* are not subject to the DPA. There are exceptions for: (i) the processing of personal data by a natural person in the course of a purely personal or household activity; and (ii) operations concerning public security, defence or state security.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to automatic processing of personal data as well as non-automatic processing of personal data that is or may be contained in a personal data filing system. A personal data filing system means any structured and stable set of personal data that is accessible according to specific criteria.

Rights of Data Subjects

Compensation

Pursuant to civil liability principles, *data subjects* have a right to compensation if they suffer damage.

Fair processing information

A *data controller* must provide *fair processing information* to *data subjects*. This also includes information as to: (i) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (ii) the identity of the recipients or the category of recipients to which the recipients belong; (iii) the existence of the right of access to and the right to rectify personal data and the right to oppose the processing; and (iv) in the case of *transborder dataflows*, information on such transfer.

It is a general obligation under French law to use the French language when conducting business or dealing with consumers or employees in France. Therefore, in most instances, this will also apply to *fair processing information*. Though the DPA does not specify that the DPA itself must be mentioned in any *fair processing information*, all information samples proposed by the CNIL include a specific reference to the DPA.

Rights to access information

Data subjects or a duly empowered representative may obtain *subject access information* by written request to *data controllers*. Such written request must be signed and an identification document must be attached. A copy of the data processed must be provided to the *data subjects* at a cost that must not exceed the cost of copying the relevant documents. The *data controller* may object to abusive queries from *data subjects*, the *data controller* being responsible for proving the abusive nature of such queries. There are also a range of statutory exceptions for certain types of processing. Some access rights are only indirect, such as, for instance, access to the list of banking accounts of the FICOBA.

Objection to direct marketing

Data subjects also have the right to object, free of charge, to the processing of their personal data for direct marketing purposes by the current or future *data controller*. The *data controller* must then cease such processing within a reasonable period.

Other rights

Data subjects also have the right to ask the *data controller* to rectify, complete, update, block or erase their data where they are incomplete, inaccurate or where the use, transfer or storage of such data is forbidden.

Data subjects have the right to object at any time to the processing of their personal data on compelling legitimate grounds. In certain cases, *data subjects* may object to decisions being taken about them based solely on automatic processing.

Security

Security requirements in order to protect personal data

The *data controller* or any person acting under his instructions must comply with the *general data security obligations*.

Specific rules governing processing by third party agents (processors)

Wherever a sub-contractor is involved (a *data processor* acting on behalf of the *data controller* being viewed as a sub-contractor), the *data controller* shall ensure that: (i) the sub-contractor presents sufficient guarantees to enable the implementation of the security and confidentiality measures and that the sub-contractor complies with the same *general data security obligations*; and (ii) the contract with the sub-contractor contains the *standard processor obligations*. The *data controller* remains in all cases jointly liable with respect to the security and confidentiality of the personal data.

Notice of breach laws

There is still no general notice of breach obligation under the DPA.

However, in accordance with the *Citizens' Rights Directive*, as transposed in the Ordinance and further detailed in Decree n°2012 436 of 30 March 2012, public network services providers must notify the CNIL without delay of any personal data breach that occurs in connection with the provision of an electronic communication service. Where such a personal data breach might impact a user's or an individual's personal data or privacy, the service provider must also notify that person without delay, unless the CNIL determines that adequate protective measures have been implemented (for example, as a result of encryption) and that the personal data breach is assessed by the CNIL as not being material. Operators must also maintain an inventory of data breaches.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the *data controller* satisfies the *standard conditions for transborder dataflow*. However, in terms of the *data subject's* consent, the CNIL considers that such consent is almost never deemed to be sufficient when the transfer relates to employees' personal data.

Additionally, while personal data can be transferred freely to EEA countries, the *data controller* must still: (i) inform the *data subject*; and (ii) file an appropriate declaration with the CNIL (which delivers a receipt enabling the transfer without delay).

Notification and approval of national regulator (including notification of use of Model Contracts)

When the *Model Contracts* are used for *transborder dataflows*, prior authorisation must be obtained from the CNIL.

Use of binding corporate rules

The CNIL has approved and is very supportive of the use of *binding corporate rules* and is part of the mutual recognition "club". Recently, the CNIL approved the *binding corporate rules* of LVMH, CMA-CGM, Hermès and Novartis. Using *binding corporate rules* for international data transfers still requires an authorisation from the CNIL.

Enforcement

Sanctions

The CNIL may issue a wide array of penalties, including: (i) a warning; (ii) a formal demand; (iii) the issuing of an injunction to cease processing; (iv) financial sanctions of up to EUR 150,000 for the first breach (and up to EUR 300,000 in the case of a repeat breach within five years); and (v) the revocation of the CNIL's authorisation. In cases of emergency, i.e. infringement of human rights, privacy rights or individual liberties, the CNIL may decide: (i) to order the cessation of processing for a maximum three-month period; (ii) to lock personal data processed for a maximum three-month period; or (iii) to inform the Prime Minister in order that appropriate security measures be taken. In cases where there is serious infringement of human rights, privacy rights or individual liberties, the president of the CNIL may ask any competent jurisdiction to take, by interim ruling, any measure necessary to prevent the infringement.

Criminal sanctions may also be imposed up to a maximum of five years' imprisonment and fines from EUR 15,000 (and up to EUR 75,000 for legal entities) to EUR 300,000 (and up to EUR 1,500,000 for legal entities).

Practice

In 2011, the CNIL received 5,738 complaints for breach of the DPA. In 2011, there were 385 investigations, 65 formal notices, 13 warnings and 5 financial sanctions imposed by the CNIL. In general, the CNIL is increasing its enforcement activity and the CNIL described investigations as a priority in its annual report. In March 2011, the CNIL issued a fine of EUR 100,000 against Google with respect to its Street View data processing. More recently, in January 2012, the CNIL issued a fine of EUR 20,000 for the sending of unsolicited commercial SMS by a real estate diagnostics company, without providing *fair processing information* or allowing the right to oppose in a simple and free of charge manner. The

CNIL has published its investigation programme for 2012 on its website, anticipating 450 on-site investigations. The CNIL is also looking at more flexible informal enforcement approaches (such as published "naming and shaming").

Enforcement authority

The CNIL has the power to take enforcement action in France. It has the ability to fine organisations itself as it may issue financial sanctions (i.e. administrative fines). The CNIL's sanctions can be made public (usually on its website) and be published in newspapers at the cost of the defaulting *data controller*. Prosecutions for criminal offences are brought before the French criminal courts, which have the power to impose criminal fines and/or imprisonment.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The "Trust in Computer Processing in the Economy Act" (the "**Act**") implemented Article 13 of the *Privacy and Electronic Communications Directive* on 21 June 2004. The Act is now codified under Article L. 34-5 of the Code of Post and Telecommunication and is mentioned in Article L.121-20-5 of the Consumption Code.

The Ordinance implements the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

The Ordinance requires *data controllers* to obtain consent from users to store or access cookies after having provided the user with information about the purposes for which cookies are used and about the means to prevent such storage or access.

The Ordinance explicitly recognised that such consent may result from appropriate settings on a user's connection device (such as an internet browser) or from any other applications placed under a user's control.

User consent is not required where the cookie's sole purpose is to enable or facilitate the communication or it is strictly necessary to provide an online communication service requested by the user.

Regulatory guidance on the use of cookies

The CNIL issued guidance about the Ordinance on 26 April 2012. It states that current browser default settings are not sufficient to provide consent.

Other means to obtain consent include: (i) use of a banner tick box at the top of a web page; (ii) an area requesting consent highlighted on a web page; or (iii) boxes to tick at the time of subscription to an online service. The CNIL considers that it is not possible to obtain consent simply by including cookie wording in the website's terms of use. Furthermore, the CNIL does not recommend pop-up windows because they are often blocked by the browser.

The CNIL also lists cookies it considers as exclusively intended to enable or facilitate communication by electronic means or strictly necessary for the provision of an online communication service at the user's express request. This includes shopping cart cookies, session cookies, cookies used for security purposes and cookies registering the language spoken by the user. However, the CNIL still recommends that users are provided with information about those cookies in the privacy policy of the website.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing e-mail requires the "prior consent" of the recipient. "Prior consent" is defined by the law as a "free, specific and informed manifestation of consent to his personal data being used for direct marketing purposes".

Conditions for direct marketing by e-mail to corporate subscribers

The law applies to individual recipients but not to company recipients.

Exemptions and other issues

It is permitted to send an e-mail for the purposes of direct marketing if it falls within the *similar products and services exemption*. The Act also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; (ii) an opt-out address is not provided; or (iii) the title of the e-mail does not relate to the service or product offered.

The sender must also include the *eCommerce information*.

SMS/MMS are subject to the rules on direct marketing by telephone rather than the rules on direct marketing by e-mail.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing by telephone or SMS/MMS requires the "prior consent" of the recipient. It is not permitted to make direct marketing calls or send SMS/MMS to individual subscribers: (i) who have previously objected to such calls; or (ii) who are ex-directory.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to make direct marketing calls or send SMS/MMS to corporate subscribers without their prior consent.

Exemptions and other issues

Calls can be made and SMS/MMS can be sent to subscribers if they have consented to receiving such calls or SMS/MMS.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax requires the "prior consent" of the recipient. It is not permitted to send direct marketing faxes to individual subscribers: (i) who have previously objected to such faxes; or (ii) who are ex-directory.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send direct marketing faxes to corporate subscribers without their prior consent.

Exemptions and other issues

The Act also prohibits direct marketing by fax from being sent if: (i) the identity of the sender is disguised or concealed; (ii) an opt-out address is not provided; or (iii) the title of the fax does not relate to the service or product offered.

Germany.

General | Data Protection Laws

National Legislation

General data protection laws

The German Federal Data Protection Act (Bundesdatenschutzgesetz) (the "**DPA**") implemented the *Data Protection Directive* into German law. This was subject to major amendments in July 2009 by the Federal Data Protection Act Amendment Law (Novelle des Bundesdatenschutzgesetzes), the majority of which entered into force on 1 September 2009.

The German legislator is currently working on a reform of employee data protection law. This new law is expected to clarify the current regime, e.g. how to treat data of applicants who were not hired; and regulate both general and specific aspects of employee data protection, e.g. allowing medical check-ups as part of application procedures (under certain circumstances). A final decision on such new legislation is yet to be taken and, according to various informal sources, it is very unlikely that the new law will come into force prior to the next general election in autumn 2013.

Entry into force

The implementing legislation came into force on 23 May 2001, and was amended on 1 September 2009.

National Regulatory Authority

Details of the competent national regulatory authority

There are 20 different federal and regional supervisory authorities responsible for monitoring the implementation of data protection. The names, addresses and websites of these supervisory authorities are available at www.datenschutz-berlin.de/content/adressen/deutschland/aufsichtsbehoerden.

Notification or registration scheme and timing

(a) In general, automated processing procedures are required to be registered with the competent supervisory authority in advance.

(b) In particular, automated processing procedures must be registered if the *data controller* commercially stores personal data for the purpose of transfer or market research.

In either case there is no charge for registration.

Exemptions

In relation to (a) above, a registration is not required if: (i) the *data controller* has appointed a data protection official (which is usually the case in Germany); or (ii) as a rule, a maximum of nine employees are permanently involved in the collection, processing or use of personal data and either consent has been obtained or the use of the data is required for the establishment, implementation or termination of a contractual obligation with the *data subject*.

In relation to (b) above, there are no exemptions.

Appointment of a data protection officer

Every private entity with: (i) more than nine persons permanently engaged in automated data processing; or (ii) at least 20 persons engaged in non-automated processing, is obliged to appoint a data protection official. The data protection official must be appointed within one month following the beginning of the data processing. Data protection officials enjoy special protection against dismissal.

Personal Data

What is personal data?

The definition of personal data in the DPA is "any information concerning the personal or material circumstances of an identified or identifiable individual". However, the requirement that the information concerns a "personal or material circumstance" is interpreted very broadly (see the Federal Constitutional Court's decision in Volkszählungsurteil) so in practice this definition is very similar to the *standard definition of personal data*.

In addition, it is commonly considered that whether or not an individual is identifiable and thus information regarding this individual might be qualified as personal data must be considered from the point of view of the person who is in possession of the information (and should not consider information held by third parties). In this respect, the German interpretation of personal data differs slightly from the *Opinion on Personal Data*.

Guidance from data protection authorities indicates that static IP addresses should be treated as personal data. In addition some authorities and some courts (see County Court of Berlin, file number: 5 C 314/06 and 23 S 3/07; County

Court of Cologne, file number: 28 O 339/07) consider dynamic IP addresses (in the hands of someone other than the individual's ISP) to be personal data though the German Federal Government and other authorities disagree.

Is information about legal entities personal data?

No. However, information about sole traders (Einzelkaufleute) and partnerships (Personengesellschaften) is personal data if, and to the extent, such information interferes with the personal circumstances of the traders and partners involved.

What are the rules for processing personal data?

Generally, personal data may be processed if one of the *standard conditions for processing personal data* is met. Additional, special requirements apply to: (i) employee data; (ii) personal data used for marketing and address trading; (iii) scoring; and (iv) market and opinion research.

Are there any formalities to obtain consent to process personal data?

Consent must be based on the *data subject's* free decision and should be in writing unless special circumstances dictate otherwise. If consent is to be given together with other declarations (for example, together with general terms and conditions), it must be made distinguishable. It is widely acknowledged that valid consent from employees is hard to obtain as the employees' dependence on the employers generally excludes the ability to make a free decision.

The proposed new employee data protection law (please see the section entitled *General data protection laws*, above) is expected to give a clear indication of situations in which consent from employees will be valid.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data means the *standard types of sensitive personal data*. Information on criminal offences is not considered to be sensitive personal data. Nevertheless, when collecting, processing or storing such information and balancing the interests of the *data subject*, information on criminal offences (in particular, criminal offences committed by employees) is treated as more sensitive than other personal data.

The DPA also has additional processing rules that apply to the processing of CCTV footage. The proposed new employee data protection law (see above) is expected to explicitly prohibit any use of CCTV in private spaces, such as rest rooms.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met.

Are there any formalities to obtain consent to process sensitive personal data?

In addition to the requirements and formalities applicable to personal data (see above), such consent must refer expressly to the sensitive personal data which will be processed.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The responsibility for complying with the provisions set out in the DPA is generally borne by the *data controller*. *Data processors* are subject to a reduced set of specific requirements such as the obligation to ensure its employees maintain confidentiality when taking up their duties. Additionally, technical and organisational measures must be agreed between the *data controller* and the *data processor*. The applicable minimum requirements regarding technical and organisational measures ensuring data security are set forth in the DPA.

Are both manual and electronic records subject to data protection legislation?

Public bodies: Yes

Private bodies: Yes. However, the DPA applies only to the extent personal data is: (i) processed or used by means of data processing systems or is collected for such systems; or (ii) processed or used in, or from, non-automatic filing systems or is collected for such systems. Employee data, however, is subject to the DPA regardless of whether such data originates from manual or electronic records.

Rights of Data Subjects

Compensation

Where a *data controller* causes harm to the *data subject* through inadmissible or incorrect collection, processing or use of his personal data, such controller or its supporting organisation must compensate the *data subject* for the harm caused.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. If the information is collected under a legal obligation or for the provision of benefits then the individual must be informed if obligation to provide information is mandatory or voluntary and of the consequences of not providing the information.

There is no obligation in the DPA to provide this information in German, though it may be difficult to show the information has been fairly provided if it is not in the language the *data subject* is familiar with. There is no obligation to refer to the DPA itself in any *fair processing information*.

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers* and such information is generally provided free of charge. If the information is stored in the course of business for transfer purposes (e.g. from a credit agency) the *data subject* may also request such information once a year free of charge. Any further information requests, however, may incur a charge.

Objection to direct marketing

The *data subject* has the right to object to personal data being transferred for purposes of advertising and market and opinion research.

Other rights

The *data subject* may demand the correction of incorrect data as well as the deletion or blocking of personal data, the storage of which is not, or is no longer, covered by legitimate purposes.

Security

Security requirements in order to protect personal data

Public and private bodies processing personal data, either on their own behalf or on behalf of others (*data processors*), are obliged to take the technical and organisational measures required to ensure compliance with the provisions of the DPA. The minimum requirements the *data controller* and the *data processor* must adhere to relate to access control, transmission control, input control, availability control and the separation of data.

Specific rules governing processing by third party agents (processors)

In the event that a *data processor* is handling personal data on behalf of a *data controller*, the *data processor* and the *data controller* need to conclude a written agreement about the commissioned processing of data which must include a specific set of minimum requirements comprising the *standard processor obligations* and additional requirements such as a description of the object and duration of the processing and an obligation on the *data processor* to notify the *data controller* of any security breaches. Where *data processors* are commissioned to handle data, the responsibility for compliance with the provisions of the DPA is borne by the *data controller*. Therefore, the *data controller* must ensure that the data is processed strictly in accordance with its instructions.

Notice of breach laws

Private entities must notify the competent regulatory authority and the persons affected if their data has been unlawfully disclosed to third parties (whether by illegitimate transfer, data leakage or hacker attack) if there is a danger of serious prejudice to the interests of the person affected (for example, the loss of credit card or patient data). If it is too difficult to directly notify all persons affected, a notice must be published in two daily newspapers.

Further notice of breach obligations apply to those providing telemedia services under the German Telemedia Act (Telemediengesetz) (the "**TMA**").

Transfer of Personal Data to Third Countries

Restrictions on Transfer to third countries

If the general provisions for the transfer of personal data set out in the DPA have been complied with, transfer of personal data to countries outside of the EEA is permissible if the transfer satisfies the *standard conditions for transborder dataflow*.

Notification and approval of national regulator (including notification of use of Model Contracts)

The DPA does not contain an obligation to notify the authority when transferring personal data to countries outside the EEA when using *Model Contracts*. However, if the *Model Contracts* are modified then approval must be sought and some of the German data protection authorities require a copy of the signed *Model Contracts* to be submitted by the data exporter.

Use of binding corporate rules

Besides the *standard conditions for transborder dataflow*, the competent authority may allow individual transfers of certain categories of personal data to non-EEA countries if adequate safeguards with respect to the protection of privacy are guaranteed. *Binding corporate rules* are a method for such protection and require approval by the competent supervisory authority. Germany is part of the mutual recognition club for *binding corporate rules*.

Enforcement

Sanctions

Should a *data controller* infringe the *data subject's* rights under the DPA, the *data subject* is entitled to injunctive relief and compensation for damages. In addition, a violation of the DPA may result in administrative fines and penalties. Fines should aim to confiscate, in particular, profits and therefore be higher than any potential economic gain resulting from the breach of the DPA.

Practice

With respect to any information about investigations and prosecutions in Germany, three things should be noted: (i) reliable information is very hard to obtain. This is due to the fact that in Germany there are several responsible authorities acting independently (please see the section entitled "*Details of the competent national regulatory authority*" above). In addition, the reports published by the various data protection authorities do not contain details of penalties imposed or the facts of the relevant cases; (ii) in Germany there is a distinction between criminal sanctions (Straftaten) and administrative fines (Ordnungswidrigkeiten) both of which are applicable in relation to data protection infringements; and (iii) the sanctions regime was significantly amended in September 2009. To date, there is no established practice under the new regime.

Generally, data protection breaches may be punished by a fine of up to EUR 50,000 per breach or, in certain cases, up to EUR 300,000 per breach. Additionally, further administrative offences have been introduced, which include deficiencies in ordering commissioned data processing (Auftragsdatenverarbeitung) and insufficient monitoring by the *data controller*.

In October 2009, however, the data protection authority of Berlin imposed a fine of EUR 1,123,503.50 on Deutsche Bahn AG because of significant violations of data protection law. This is the highest administrative fine ever imposed in Germany due to non-compliance with data protection law.

Enforcement authority

The various federal and state data protection authorities in Germany have the power to take enforcement actions. They themselves (or in co-operation with other administrative authorities) may: (i) fine organisations (administrative fines); (ii) order that any discovered breaches be remedied; and (iii) in the event of serious infringements, ban certain procedures.

However, prosecutions for criminal offences must be brought before the German Criminal Courts (by public prosecutors) who can impose fines or imprisonment.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The German Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb) (the "**UCA**") dated 3 July 2004 and the revised German Telecommunications Act (Telekommunikationsgesetz) (the "**TA**") dated 22 June 2004 (with the TA being applicable only to telecommunications service providers in addition to the UCA) both implemented Article 13 of the *Privacy and Electronic Communications Directive*. Further, the TMA may be amended to implement the *Citizens' Rights Directive* as regards the storage of cookies.

Cookies

Conditions for use of cookies

Consent is only needed for the use of cookies referring to personal data.

Regulatory guidance on the use of cookies

The TMA does not expressly refer to the use of cookies. However, there is an express requirement for consent for the use of personal data, which includes cookies referring to personal data, to be given "prior" to such use.

The TMA may be amended to implement the *Citizens' Rights Directive*. A draft bill, published in June 2011, foresees the necessity to obtain consent to store any cookies on the user's terminal equipment unless the cookie is strictly necessary for the provision of a service to that subscriber or user. However, the German government has – against the view of the

supervisory authorities – recently taken the position that, due to the already existing provisions of the TMA, no changes are required.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing via e-mail principally requires the prior explicit consent of the recipient.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing via e-mail principally requires the prior explicit consent of the recipient. The Federal Court of Justice recently confirmed that a single unsolicited e-mail sent to a corporate subscriber infringes the applicable law (Federal Court of Justice, file number: I ZR 218/07).

Exemptions and other issues

The *similar products and services exemptions* apply.

The UCA, however, also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) if an opt-out address is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Individual calls (without the use of automated calling systems) to individual subscribers who are consumers for the purposes of direct marketing are subject to the explicit prior consent of the subscriber.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Individual calls to corporate subscribers (and individuals who are not acting in their capacity as consumers) are only possible with their explicit or implied consent. Hence, in contrast to calls vis-à-vis consumers, implied consent is sufficient. However, German case law indicates that such an implied consent is subject to quite strict requirements.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The use of fax for the purposes of direct marketing is only allowed in respect of individual subscribers (i.e. consumers) who have given their prior explicit consent.

Conditions for direct marketing by fax to corporate subscribers

The use of fax for the purposes of direct marketing is only allowed in respect of corporate subscribers who have given their prior explicit consent.

Exemptions and other issues

No exemptions apply.

Greece.

Contributed by Karageorgiou & Associates Law Firm

General | Data Protection Laws

National Legislation

General data protection laws

The Data Protection Act (Law 2472/1997), as amended by Law 3471/2006 (G.G. 133A'/28.06.06) and Law 3625/2007 (G.G. 290A'/24.12.2007), (collectively, the "**DPA**") implemented the *Data Protection Directive*.

Entry into force

The DPA came into force on 10 November 1997.

National Regulatory Authority

Details of the competent national regulatory authority

Data Protection Authority (the "**Authority**")
1-3 Kifisias Avenue
Ampelokipi 115
Athens
Greece

www.dpa.gr

Notification or registration scheme and timing

The *data controller* must notify the Authority in writing of the establishment of a filing system and the commencement of a data processing activity. There is no charge for notification and no approval by the Authority is required. The notification must take place before the commencement of any data processing activities.

However, the processing of sensitive personal data requires a special authorisation issued by the Authority following the submission of the relevant application. The authorisation is given for a specific period of time, depending on the purpose of the data processing and it may be reviewed upon request of the *data controller*. Authorisation costs between 30 EUR and 90 EUR for natural persons and 300 EUR and 900 EUR for legal persons. Processing can only commence once the authorisation is given and any change in the data referred to in the authorisation should be communicated without undue delay to the Authority.

Exemptions

The *data controller* is exempt from the obligations of notifying the Authority and obtaining permits where: (i) processing is carried out exclusively for purposes directly relating to an employment or project relationship or the provision of services to a public authority and is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationships, provided that the *data subject* has been notified; (ii) processing relates to clients' or suppliers' personal data, provided that such data are not disclosed to third parties and excluding entities whose main activities involve trading of data, credit and financial institutions, or pharmaceutical and insurance companies; (iii) processing is carried out by societies, enterprises, associations and political parties about their members and those members have given consent and the data are not disclosed to third parties; (iv) processing is carried out for medical purposes by persons subject to obligations of professional secrecy; (v) processing is carried out by lawyers, notaries, unpaid land registrars and court officers and relates to the provision of legal services to their clients; and (vi) processing is carried out by judicial authorities or services in the framework of attributing justice or for their proper operational needs.

Appointment of a data protection officer

There is no general legal requirement to appoint a data protection officer. However, the description of each data file should include information on the person responsible for the processing of personal data in order for the *data subjects* to exercise their rights under the DPA.

Personal Data

What is personal data?

Personal data means any information relating to the *data subject*, but consolidated data of a statistical nature, from which *data subjects* can no longer be identified, is not considered to be personal data. Therefore, the definition of personal data in the DPA is closely based on the *standard definition of personal data*.

The Authority has not adopted specific guidance but uses a broad approach to the definition of personal data in line with the *Opinion on Personal Data* in its decisions. One example is the Authority's Decision 91/2009 on personal data

collected by a company providing three-dimensional virtual navigation services. The Authority suggested that the combination of internet geographical mapping applications (such as Google maps) with information included in publicly available directories (such as the address in telephone directories) can lead to the identification of persons and result in the attribution of certain physical, economic or social characteristics to them.

Is information about legal entities personal data?

The DPA applies to individuals only. Legal persons may, however, be entitled to data protection rights under Article 9A of the Greek Constitution and Articles 57, 59 and 932 of the Greek Civil Code, which relate to the protection of personality.

The DPA applies to sole traders and partnerships, where data on such legal entities relates to a natural person, (for example, where the trade name of a partnership is the name of a natural person).

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. However, in practice, the legitimate interest condition is not frequently relied upon as the *data controller* must establish that a number of onerous criteria are satisfied.

The DPA does not apply to the processing of personal data carried out: (i) by a natural person for a purely personal or household activity; (ii) by judicial-public prosecution authorities for the administration of justice, especially for crimes punished as felonies with intent against life, personal and sexual freedom, crimes involving the economic exploitation of sexual life, crimes against property, drugs, and plotting against public order, as well as crimes against minors and especially for data collected by the recording of sound or image through technical devices for the administration of justice; or (iii) by public authorities, under the authorisation of the public prosecutor, where public order and security are at serious risk and the aim is to provide evidence of the commitment of crimes.

Are there any formalities to obtain consent to process personal data?

Consent should be express and can only follow from the *data subject* receiving proper written information regarding the data processing. According to opinion no. 115/2001 of the Authority, it is difficult for an employer to prove that employees have freely given consent due to the imbalance of power between the parties resulting from the employment contract. Where employees' consent is considered freely given, it can only be provided for precisely determined purposes. It is forbidden to collect or process employee personal data for purposes not directly or indirectly involved with the employment relationship, irrespective of the employee's consent.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes: (i) *standard types of sensitive personal data;* (ii) information about social welfare; (iii) information about membership of societies; and (iv) information about criminal offences or criminal proceedings.

Biometric data is not explicitly included in the category of sensitive personal data of the DPA, however, if it reveals information such as ethnic origin or health, it is considered sensitive personal data.

In decision 23/2008, the DPA concluded that information about a person's participation in a Masonic Lodge was sensitive personal data, irrespective of societal opinion regarding the principles of Freemasonry.

Are there additional rules for processing sensitive personal data?

The processing of sensitive personal data requires a permit from the Authority. Following the submission of the request, the Authority may summon the *data controller*, his representative, and the *data processor*, to a hearing before issuing a permit for data processing.

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met, however, there are further legal obligations imposed in the field of employment law and on non-profit seeking bodies in relation to the data categories (ii)-(iv) above.

In addition to the standard conditions for processing sensitive personal, the DPA allows the processing of sensitive personal data: (i) for reasons of national security, crime, public health and the exercise of public control on fiscal or social services, provided the processing is carried out by a public authority; (ii) for research or scientific purposes, provided anonymity is granted; and (iii) pertaining to public figures for journalistic purposes, provided that such data are in connection with the holding of a public office or the management of third parties' interests.

Publication of information regarding criminal offences by the Public Prosecutor's Office is also permitted in certain circumstances.

If the collection and processing of data regarding criminal offences is necessary for certain employment posts, it will be legitimate and lawful only if: (i) the type of data is directly related to the specific employment; (ii) the processing is

absolutely necessary for reaching a decision within the specific employment (for example, the criminal record of employees managing money); and (iii) the data are collected directly from the employee or candidate.

Sensitive personal data related to employees' health can be lawfully collected, provided: (i) the data are collected directly from the employee or candidate; and (ii) the data are absolutely necessary for the evaluation of employee suitability, health and safety, or the establishment of employees' rights and social benefits. The analysis of human genetic data is prohibited in an employment relationship as this constitutes a radical offence of personality.

Are there any formalities to obtain consent to process sensitive personal data?

Consent to processing sensitive personal data must be obtained in writing.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*. If the *data controller* is not established on the EU territory it must, in a written statement to the Authority, designate a representative established in the Greek territory. The same shall also apply when the *data controller* is subject to exterritoriality, immunity or any other reason inhibiting criminal prosecution.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. The *data controller* can be a natural or legal person, public authority, agency or any other organisation. *Data processors* are not subject to the DPA, but they should comply with the *standard processor obligations*.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to the processing of personal data: (i) by automatic means, in whole or in part; and (ii) by non-automatic means provided the data form part of a file or are intended to form part of a file.

Rights of Data Subjects

Compensation

The DPA provides *data subjects* with a right to compensation if they suffer damage or distress as a result of unauthorised data processing, this includes pecuniary and non pecuniary damage.

In case no. 476/2009, the Supreme Court confirmed that compensation for non pecuniary damage is available to a *data subject* for the distress caused by the unlawful processing of its personal data. The compensation is set at EUR 5,865 unless the plaintiff claims a lower amount or the said breach was due to negligence.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. This includes notifying the *data subject* of the existence of the *data subject's* right to *subject access information* and details of the recipients or categories of recipients of such data. Fair processing notices must be provided in Greek, but do not need to refer to the DPA.

Decision 21/2008 of the Hellenic Data Protection Authority confirms that providing prior written notice of the *fair processing information* to the *data subject* by the *data controller* is absolutely necessary for the fair processing of personal data.

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. According to article 12 of the DPA, the *data subject* should be entitled to request and obtain from the *data controller*, without undue delay: (i) all the personal data relating to him; (ii) the source of such information; and (iii) any kind of change in processing since he was last notified. However, according to several decisions of the Greek Authority, a cost (such as EUR 10 for reproduction costs) may be imposed on *data subjects* for gaining access to such data collected by public organisations, such as the Supreme Council for Civil Personnel Selection (ASEP) or the University Entrance Examinations (Authority's Decisions no. 40/2006 and 66/2006).

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stops processing data for unsolicited sales and marketing messages by surface mail (brochures, leaflets, etc.). The Authority keeps a register of *data subjects* who have made such requests, a so-called "Robinson's List", and the *data controllers* of the relevant files must consult this register prior to any processing and delete any listed persons from their files. Separate restrictions apply to email (see **Marketing by Email**, below).

Other rights

Data subjects may request that their data be rectified.

A *data subject* may require in writing that the *data controller* cease processing. The right to object includes provisional non-utilisation, locking, non-transmission or deletion.

A *data subject* can seek provisional judicial protection from the competent court, such as immediate suspension or non-application of an act or decision affecting the *data subject*, issued by an administrative authority or public law entity or association or natural person solely on automated processing of data, intended to evaluate the subject's personality, effectiveness at work, creditworthiness, reliability and general conduct.

Security

Security requirements in order to protect personal data

Data controllers must comply with the *general data security obligations*. The DPA has the authority to issue specific regulations with regard to security measures and use of technological measures for the protection of personal data. These measures should protect personal data and maintain its quality. For this reason, *data controllers* should take all appropriate technical, physical and organisational measures to protect personal data against unauthorised access, unlawful processing, accidental loss or damage or unauthorised destruction (e.g. physical access control, CCTV, biometrical techniques, secure information system firewalls, security patching and threat analysis).

Specific rules governing processing by third party agents (processors)

The *data processor* must fulfil certain professional qualifications and provide sufficient guarantees in respect of technical expertise and personal integrity to ensure confidentiality. If the *data processor* is not dependent upon the *data controller* (i.e. is not an employee of the *data controller*), there must be a written contract containing the *standard processor obligations.*

Notice of breach laws

There is no express requirement under the DPA to notify the Authority or *data subjects* of general data breaches of the DPA. However, when imposing fines the Authority takes into consideration whether a breach was notified on a voluntary basis. In Decision 87/2011 no fine was imposed when a prompt notification was made to the Authority and in Decision 60/2011 no fine was imposed because: (i) it was the company's first data breach; (ii) the company took measures to minimise the impact of the data breach; and (iii) the company voluntarily notified the Authority of the breach.

In the electronic communication sector, the legal requirement for the provision of notice of breach laws ("**Data Breach Notification**") is established by Law 3471/2006 (as amended by Law 4070/2012 implementing the *Citizens' Rights Directive*).

Moreover, the Bank of Greece Governor's Act no. 2577/2006 (implementing Directive 2006/73/EC – MIFID – Level II), imposes an obligation on banks and financial institutions to set up a policy to notify customers in case of breach of their personal data.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA prohibits transfers outside of the EU unless the transfer satisfies the *standard conditions for transborder dataflow*. Where the transfer: (i) is to a *whitelisted country*; (ii) is made pursuant to a set of *Model Contracts*; or (ii) the recipient of the data participates in the US Safe Harbor, the *data controller* should simply notify the Authority about the data transfer.

However, where: (i) data are transferred on the basis of *binding corporate rules*; (ii) the *data subject* has consented to such transfer; (iii) the transfer is necessary for the performance of a co-operation agreement with the public authorities of another country and under condition that the *data controller* provides adequate safeguards with respect to the protection of the *data subjects'* privacy; or (iv) the transfer is necessary for the establishment, exercise or defence of a right in court, the *data controller* should apply to the Authority for an authorisation confirming that the country of destination of data provides an adequate level of protection.

Notification and approval of national regulator (including notification of use of Model Contracts)

If the transfer is not to an adequate country, special permission is required from the Authority.

In case that a data transfer is based on Model Clauses such transfer must be notified but does need to be approved by the Authority.

Use of binding corporate rules

The Greek Authority recognises the use of *binding corporate rules* in Greece. Nevertheless, as of the end of 2012, no transfer of personal data outside the EU has been approved based on *binding corporate rules*.

Enforcement

Sanctions

Breach of the specific provisions of the DPA carries consequences of an administrative, criminal and civil nature.

The Authority may issue a wide array of penalties including: (i) a warning with a deadline to stop the breach, (ii) fines ranging from EUR 880 to EUR 150,000; (iii) temporary or permanent revocation of licences; and (iv) destruction of a filing system or interruption of processing and destruction, return or blocking of the relevant files.

Criminal sanctions may also be imposed up to a maximum of ten years' imprisonment and fines from EUR 2,940 to EUR 14,680 (i.e. imprisonment and imposition of fines). If the offence is committed by a *data controller* that is a legal entity, the natural person who legally represents the legal entity is lawfully responsible.

Independently of any criminal liability, the *data subject* whose rights have been infringed is entitled to injunctive relief and compensation for damages he has suffered due to the *data controller's* acts or omissions. If the loss is not financial, the *data subject* may be awarded punitive damages. The DPA imposes a standard of liability that is close to strict, in the sense that the person causing the loss will not be excused simply because he or she was unable to predict the loss.

Practice

There are no official statistics on the number of investigations, claims and prosecutions concerning violations of the DPA, since the Authority has not published an Annual Report for 2011-2012. However, pursuant to information available on its website, during 2012, the Authority's investigations were mainly focused on financial institutions and banks with regard to security measures included in their IT systems for the destruction of their clients' personal data, as well as their failure to satisfy *data subject's* rights to access their data and object to their collection.

Amongst the highest penalties imposed were: (i) EUR 50,000 imposed on a Greek bank for the issuance and delivery of a credit card to a consumer without his prior consent; (ii) EUR 50,000 imposed on a Greek bank for failure to destroy its clients' data following the lapse of their retention period; (iii) EUR 50,000 imposed on a Greek bank for the unlawful disclosure of its clients' financial data to a credit reference agency; and (iv) EUR 30,000 imposed to a Greek electronic communication provider for its failure to satisfy the *data subject's* right to delete his data.

Enforcement authority

The Authority has the power to take direct enforcement action in Greece. It has the authority to issue enforcement notices as well as the ability to fine organisations itself. The Authority's resolutions can be appealed before the Courts, which in most cases confirm such resolutions. Prosecutions for criminal offences are brought before the Greek Criminal Courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Law 3471/2006 (G.G. 133A'/28.06.06) under the title "Protection of privacy and personal data in the telecommunications sector" (the "**Law**") implemented the *Privacy and Electronic Communications Directive* and was subsequently amended by Law 3783/2009 (G.G. 136/0A'/07.08.09) and Law 4070/2012 (G.G. A-82/10.04.2012) which implemented the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Under Law 3471/2006 (as amended by Law 4070/2012) cookies (or similar technologies) can be used to store information or gain access to information stored in the technical equipment of the subscriber/user on condition that he/she has given his/her consent, having being provided with clear and comprehensive information about cookie use.

The Law recognises the possibility of obtaining consent via browser or other application settings.

Exceptionally, consent is not required for technical storage or access for the sole purpose or carrying out the transmission or a communication through an electronic communication network, or when strictly necessary for the provision of information society services explicitly requested by the subscriber/user ("'Cookie Consent Exemption").

Regulatory guidance on the use of cookies

The Authority clarifies that, if consent is obtained via browser or other application settings, the *data subject's* consent should be requested for every single cookie to be installed and a general and abstract consent to all cookies provided by the *data subject* a priori via browser or other application settings is not valid.

The Authority follows the Article 29 Working Party Opinion 4/2012 on Cookie Consent Exemption with regard to session cookies, persistent cookies, authentication cookies, social plug-in content cookies etc.

Furthermore the Authority clarifies that cookies installed for the purpose of online advertising are expressly exempted from the Cookie Consent Exemption and the *data subject* should explicitly provide his/her consent for installation of both 'first party cookies' and 'third party cookies'.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under Article 11 of the Law it is not permitted to transmit the unsolicited direct marketing of goods or services through e-mail unless the recipient has previously notified the sender that he consents for the time being to such communications being sent by the sender. However, paragraph 2 of the same Article provides that unsolicited communications are generally prohibited if natural or legal persons have been registered to so-called "opt-out registers".

Under Directive 2/2011 of the Greek Authority, subscribers/users can provide their consent in writing or by electronic means. When consent is provided by electronic means the "double opt-out procedure" should be followed. Once subscribers/users have provided their consent to receiving e-mails for marketing purposes, the *data controller* should confirm that such consent has actually been provided. The *data controller* should therefore send a request for confirmation to the subscriber/user who must take some action to confirm that he/she is the owner of that email address, that the address is working and that he/she actually had the intention to provide such consent. The request for confirmation should include the purpose for which it has been sent, the identity of the *data controller* and all relevant information about the data processing and it should also provide the *data subject* with the right to opt-out.

In addition to the above, the *data controller* should: (i) provide appropriate and adequate information to the subscriber/user prior to his/her consent; (ii) record the *data subject's* consent in a secure manner; (iii) make such record of consent accessible to the subscriber/user upon his/her request; (iv) provide the subscriber/user with the right to revoke his/her consent; (v) keep the relevant record as long as commercial communication is sent to the subscriber/user; and (vi) in the case that the *data controller* stops sending e-mails for direct marketing purposes subscribers/users' consent should be kept no longer that 6 months following the last e-mail.

Conditions for direct marketing by e-mail to corporate subscribers

The regime above applies to any personal e-mail addresses at corporate subscribers, e.g. papadopoulos.m@company.gr.

Exemptions and other issues

The *similar products and services exemption* applies under Article 11 § 3 of the Law 3471/2006, Article 4 of Law 2251/1994 (regarding Consumer Protection) as well as Article 6 of Presidential Decree 131/2003 (implementing the eCommerce Directive 2000/31/EC). The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided.

The sender must also include the *eCommerce information* (as per article 6 of the Presidential Decree nr. 131/2003).

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to individual subscribers who have either: (i) previously objected to such calls; or (ii) are listed on the opt-out registers.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to corporate subscribers who have either: (i) previously objected to such calls; or (ii) are listed on the opt-out registers.

Exemptions and other issues

Calls can be made to a subscriber who is listed on the opt-out registers if they have consented to receiving such calls.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send direct marketing faxes to individual subscribers who have either: (i) previously objected to such calls; or (ii) are listed on the opt-out registers.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to make direct marketing calls to corporate subscribers who have either: (i) previously objected to such calls; or (ii) are listed on the opt-out registers.

Exemptions and other issues

Faxes can be sent to a subscriber who is listed on the opt-out registers, if they have consented to receiving such faxes.

Hong Kong.

General I Data Protection Laws

National Legislation

General data protection laws

The Personal Data (Privacy) Ordinance ("**PDPO**") which contains the Data Protection Principles ("**DPP**").

Entry into force

The majority of the provisions of the PDPO came into force on 20 December 1996. The PDPO was significantly updated by the Personal Data (Privacy) (Amendment) Ordinance 2012 (the "**Amendment Ordinance**"). The majority of the provisions of the Amendment Ordinance came into force on 1 October 2012. Provisions establishing a new direct marketing regime have been gazetted to come into force in April 2013.

National Regulatory Authority

Details of the competent national regulatory authority

Office of the Privacy Commissioner for Personal Data (the "**Privacy Commissioner**")

12/F, 248 Queen's Road East

Wanchai

Hong Kong

http://www.pcpd.org.hk

Notification or registration scheme and timing

There is no legal requirement to notify the Privacy Commissioner in respect of any collection or use of personal data.

Exemptions

Not applicable.

Appointment of a data protection officer

DPP1 implicitly requires the appointment of a data protection officer to whom data access and data correction requests can be sent.

Personal Data

What is personal data?

The PDPO defines personal data to mean any data relating directly or indirectly to a living individual from which it is practicable for the individual to be directly or indirectly identified. Personal data must also be in a form in which access to, or processing of, the data is practicable.

Is information about legal entities personal data?

No. However, information about sole proprietors and partnerships may be treated as individual data if such information satisfies the definition of personal data.

What are the rules for processing personal data?

Data users are required to comply with the six data protection principles.

DPP1 provides for the lawful and fair collection of personal data and sets out the information a data user must give to a *data subject* when collecting personal data from that subject. DPP2 provides that personal data should be accurate, up-to-date and kept no longer than necessary. DPP3 provides that personal data should only be used for the purposes for which they were collected or a directly related purpose unless the *data subject* gives prescribed consent. DPP4 requires appropriate security measures to be applied to personal data. DPP5 requires that data users provide general information about the kinds of personal data they hold and the main purposes for which personal data are used. DPP6 provides for *data subjects* to have rights of access to and correction of their personal data.

A data user is required to obtain the "prescribed consent" of the *data subject* if the data user intends to use the personal data for purposes other than those for which the data were originally collected or for a directly related purpose.

Are there any formalities to obtain consent to process personal data?

Prescribed consent is defined in the PDPO to mean the express consent of the *data subject* which has been given voluntarily and not withdrawn in writing.

Sensitive Personal Data

What is sensitive personal data?

There is no concept of "sensitive" personal data under the PDPO.

However, the Privacy Commissioner has issued two Codes of Practice setting out specific requirements in respect of certain types of personal data such as identity card numbers, personal identifiers and consumer credit data. The Privacy Commissioner has also indicated that biometric data should only be collected where it is necessary and with the consent of the *data subject*.

Are there additional rules for processing sensitive personal data?

In addition to complying with the DPPs, the Codes of Practice set out additional requirements in respect of the collection, use, retention and deletion of specific types of personal data.

Are there any formalities to obtain consent to process sensitive personal data?

No. Where consent of the *data subject* is required, prescribed consent of the *data subject* would suffice. While consent can be written or oral, it is advisable to obtain the written consent of the *data subject*. Implied consent is likely to be insufficient.

Scope of Application

What is the territorial scope of application?

The PDPO applies where the data user in question controls the processing of data in or from Hong Kong even if the data processing cycle occurs outside Hong Kong. The PDPO does not contain any provisions conferring extra-territorial application.

Who is subject to data protection legislation?

The PDPO requires all "data users" to comply with the DPPs.

However, a person who merely holds, processes or uses personal data solely on behalf of another person but not for his/her own purposes is not considered to be a data user in respect of such personal data (e.g. an internet service provider who merely provides internet connection services to data users).

Are both manual and electronic records subject to data protection legislation?

The PDPO applies to both manual and electronic records.

Rights of Data Subjects

Compensation

Data subjects have a right to bring proceedings in court to seek compensation for damage, including damages for injury to feelings.

Fair processing information

Where personal data is collected from the *data subject*, all practicable steps shall be taken to ensure that the *data subject* is informed of the purpose for which the data are to be used and the classes of persons to whom the data may be transferred. The *data subject* must also be informed of his/her rights to request access to and the correction of the data and the name or job title, and address, of the individual who is to handle any such request made to the data user.

Rights to access information

Under DPP6, *data subjects* are entitled to request access to personal data within a reasonable time for a fee. There is no specified form or mode in which such request has to be made.

Data subjects are also entitled to lodge a formal "data access request": (i) to be informed by a data user whether the data user holds personal data of which the individual is the *data subject*; and (ii) to be supplied with a copy of such data. Failure to comply with a data access request is an offence under the PDPO.

Objection to direct marketing

A *data subject* may request that a data user cease to use his/her personal data for direct marketing without charge. A data user must comply with such a request.

The Amendment Ordinance includes provisions that introduce a new regime in respect of the use of personal data for direct marketing. This regime is, tentatively, set to come into force in April 2013. Under the new regime, before a data user may use or provide a *data subject's* personal data to others for use in direct marketing, the data user must obtain the *data subject's* consent or "no objection" to the intended use or provision. Accordingly, a *data subject* may object to any intended use of his/her personal data for direct marketing at this early stage. Under this regime, a *data subject* may

request that a data user cease to use his/her personal data for direct marketing in respect of which he/she had previously consented. A data user must comply with such a request.

Other rights

Under DPP6, *data subjects* are entitled to request the correction of personal data without charge to the *data subject*. This data correction request must be preceded by a data access request. There is no particular form or mode in which a data correction request has to be made.

Under provisions of the Amendment Ordinance that are yet to become effective, the Privacy Commissioner may, at his discretion and depending on the circumstances, grant assistance including arranging for legal representation of and advice to *data subjects* in respect of their legal proceedings against data users. Provisions relating to this legal assistance scheme will take effect on a date to be announced by the Government.

Security

Security requirements in order to protect personal data

Under DPP4, all practicable steps must be taken to ensure that personal data held by a data user are protected against unauthorised or accidental access, processing, erasure, loss or use. The Privacy Commissioner has recommended the use of encryption in respect of electronic data.

Specific rules governing processing by third party agents (processors)

There is no direct regulation of *data processors*. Instead, a data user is liable for its agent's or contractor's breach of the requirements under the PDPO. Further, under DPP2 and DPP4, if a data user engages a *data processor* (whether within or outside of Hong Kong), the data user must use contractual or other means to ensure that personal data is protected from unauthorised or accidental access, processing, erasure, loss or use, and is not retained for longer than necessary for the purpose of processing the data.

The Privacy Commissioner (in a non-binding guidance note issued in September 2012) has indicated that the types of contractual obligations that could be imposed on a *data processor* include that: (i) the *data processor* must not use or disclose personal data for any purpose other than for the purpose for which the personal data has been entrusted to it by the data user; (ii) the *data processor* must take certain security measures to protect the personal data entrusted to it by the data user; (iii) the *data processor* must comply with the DPPs; (iv) the *data processor* must return or delete the personal data when it is no longer required for the purpose for which it is entrusted by the data user; (v) sub-contracting be prohibited or restricted; and (vi) audit and inspection rights be provided in favour of the data user. The Privacy Commissioner has also indicated that "other means" of ensuring compliance by a *data processor* may include ensuring that reputable *data processors* are selected by a data user and that sufficient due diligence is done by a data user on potential *data processors*.

Additionally, a data user in the banking or insurance sector, in respect of any outsourcing of their business functions must, among other requirements: (i) ensure that anyone to whom it outsources any processing has appropriate controls in place to protect customer personal data; and (ii) notify its customers in general terms that their data will be transferred to an outsourcing partner.

Notice of breach laws

Although there is no legal requirement for the data users to inform the regulator of a breach of the requirements, the Privacy Commissioner issued a guidance note in June 2010 encouraging data users to notify the following parties in response to a data breach: (i) the affected *data subjects*; (ii) the Privacy Commissioner; (iii) the relevant law enforcement agencies and regulators; and (iv) such other parties who may be able to take remedial actions to protect the personal data privacy and interests of the *data subjects* affected. It is advisable for the data user to take active remedial steps to lessen the damage that a data breach may cause to *data subjects*. The guidance note (which is non-binding) sets out some other general suggestions by the Privacy Commissioner of how a data breach could be handled.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

No. There are restrictions in section 33 of the PDPO, but they have not come into effect. However, data users are required to comply with the general requirements of the PDPO, including DPP3 when transferring personal data overseas (i.e. the transfer must be for a purpose for which the data were to be used at the time of the collection of the data or a directly related purpose).

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no requirement to either notify or obtain the approval of the Privacy Commissioner.

Use of binding corporate rules

Not applicable.

Enforcement

Sanctions

Breaches of the PDPO may lead to a variety of civil and criminal sanctions including fines and imprisonment.

If a data user breaches an enforcement notice issued by the Privacy Commissioner, it will be liable to a fine of HK$50,000 (on first conviction) or HK$100,000 (on a subsequent conviction) and imprisonment for two years.

From the commencement of the provisions of the Amendment Ordinance in respect of direct marketing, the use of personal data in direct marketing without the *data subject's* consent will be a criminal offence punishable by a fine of HK$500,000 and imprisonment for up to three years. A company that provides (for consideration) a third party with personal data for the purposes of direct marketing will be liable to fines of up to HK$1,000,000 and imprisonment for up to five years. These increased sanctions are, tentatively, set to come into force in April 2013.

Practice

In recent years, a majority of complaints received by the Privacy Commissioner have involved the unlawful use or disclosure of personal data beyond the scope of collection purpose and without the consent of the *data subject*. During that period, the Privacy Commissioner also carried out extensive investigations on direct marketing practices in banking and other sectors, which in part led to the enactment of the Amendment Ordinance. However, since the enactment of the PDPO, the Hong Kong courts have not imposed any imprisonment sentence or awarded any compensation to *data subjects* for breaches of the PDPO.

Enforcement authority

The Privacy Commissioner can issue an enforcement notice, the breach of which is a criminal offence. However, the Office of the Privacy Commissioner for Personal Data does not have any criminal investigation and prosecution powers nor is the Privacy Commissioner able to award compensation to *data subjects*. The actual criminal prosecution must be brought before the Hong Kong criminal courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

There are no ePrivacy laws as such, but the PDPO does contain provisions on direct marketing.

Cookies

Conditions for use of cookies

There are no specific laws on cookies. However, if the cookies contain any personal data, the data user is required to take all practical steps to ensure that the *data subject* is explicitly informed on or before the collection of data of the purpose for which the data is to be used and the classes of person to whom the data may be transferred. This may be done either through an online notification that appears before the data collection begins or through the website's privacy statement.

Regulatory guidance on the use of cookies

The view of the Privacy Commissioner is that a cookie, in and of itself, does not ordinarily satisfy the definition of personal data under the PDPO. In order to determine whether cookies are personal data, it depends on whether the cookies contains any data that can identify an individual or whether they are held or used with other personal identifying information.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

A *data subject* may request that a data user cease to use his/her personal data for direct marketing without charge. A data user must comply with such a request. Further, the Privacy Commissioner has issued a guidance note on direct marketing. In general, the Privacy Commissioner is of the view that a data user may only use personal data for direct marketing of those products/services that are directly related to the original purpose of collection of the data (e.g. a bank may use personal data of its customers for marketing financial and insurance products).

The Amendment Ordinance includes a new regime that will replace the current "opt out" regime with a new "opt in" approach in respect of the use of personal data for direct marketing. This regime is, tentatively, set to come into force in April 2013. Under the new regime, before a data user may use or provide a *data subject's* personal data to others for use in direct marketing, the data user must: (i) inform the *data subject* of the intention to use or provide his/her personal data for direct marketing and that the data user may not use or provide the data for that purpose without the *data subject's* consent; (ii) provide the *data subject* with specific information about the kinds of personal data to be used and the

classes of marketing subjects in relation to which the data is to be used and, if the data is to be provided to others, the classes of person to which the data will be provided and whether the data will be provided for gain; and (iii) provide the *data subject* with a means (at no cost to the *data subject*) to communicate the *data subject's* consent (which is revocable) or "no objection" to the intended use or provision. If a *data subject* has consented orally to a data user using his/her personal data for direct marketing, the data user must send a written confirmation to the *data subject*, within 14 days, confirming: (i) the date of receipt of consent; (ii) the permitted kind of personal data; and (iii) the permitted class of marketing subjects.

Conditions for direct marketing by e-mail to corporate subscribers

The PDPO does not apply to corporate subscribers.

Exemptions and other issues

When a data user uses the personal data of a *data subject* for the first time for direct marketing, a data user is required to inform the *data subject* that he may, without charge to the *data subject*, opt out of the direct marketing. If the *data subject* so requests, the data user must cease to use the data without charge to the *data subject*.

The conditions on use of personal data for direct marketing imposed by the new regime imposed by the Amendment Ordinance will not apply: (i) in certain circumstances, to personal data collected prior to the effective date of the new regime; or (ii) to direct marketing companies that use personal data at the direction of a third party who has notified them that all required consents have been obtained.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The conditions are the same as for marketing by email.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The PDPO does not apply to corporate subscribers.

Exemptions and other issues

The exemptions are the same as for marketing by email.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The conditions are the same as for marketing by email.

Conditions for direct marketing by fax to corporate subscribers

The PDPO does not apply to corporate subscribers.

Exemptions and other issues

The exemptions are the same as for marketing by email.

Hungary.

Contributed by Andrékó Kinstellar Ügyvédi Iroda

General | Data Protection Laws

National Legislation

General data protection laws

Act No. CXII of 2011 on the right to informational self-determination and on the freedom of information (the "**DPA**") governs general data protection and freedom of information matters in Hungary as of 1 January 2012. The DPA implements the *Data Protection Directive*.

Entry into force

The DPA entered into force on 1 January 2012.

National Regulatory Authority

Details of the competent national regulatory authority

The National Data Protection and Freedom of Information Authority (the "**Authority**").

Mailing address: H-1530 Budapest, Pf. 5., Hungary

Address: 22/c Szilágyi Erzsébet fasor, H-1125 Budapest, Hungary

http://naih.hu

Notification or registration scheme and timing

Any data processing must be notified in the data protection register kept by the Authority. The *data controller* must file an application for registration prior to the commencement of the data processing activity. The application is subject to a fee.

Exemptions

Data controllers do not have to apply for registration for the following types of data processing operations: (i) when processing concerns the data of the *data controller's* employees, members, students or clients (with the exception of clients of financial institutions, public utilities and electronic telecommunication service providers); (ii) when processing is carried out in accordance with the internal rules of a church or other religious organisation or religious community; (iii) if processing concerns the personal data of a person receiving health care services, for the purposes of medical treatment and preventive measures or for settling social security claims; (iv) where the data contain information concerning the provision of financial and other social support to the *data subject*; (v) where the data contain the personal data of persons implicated in official regulatory, public prosecutor or court proceedings to the extent required for such proceedings; (vi) if the data contain personal data used for official statistical purposes, provided that there are adequate guarantees that the data are rendered anonymous in such a way that the *data subject* is no longer identifiable; (vii) where the data contain data of organisations and bodies falling under the scope of the Act No. 185 of 2010 on Media Services and Mass Communication, if such data are used solely for such organisations' and bodies' own purposes; (viii) if the processing serves the purposes of scientific research, provided that the data are not made available to the public; or (ix) if it concerns documents deposited in archive.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer unless the *data controller* operates in certain specified sectors (for example, financial institutions, telecommunications service providers and public utility service providers).

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. In this respect, it only applies to information about natural persons and the information remains personal data as long as its relationship with a private individual can be maintained.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if: (i) the processing is carried out with the *data subject's* explicit consent; (ii) the processing is permitted by an act of parliament or decree of a local municipality based on an act of parliament; (iii) obtaining the *data subject's* consent is impossible or would incur disproportionate expense; (iv) processing is necessary for compliance with a legal obligation pertaining to the *data controller*; or (v) processing is necessary for the enforcement

of the legitimate interests of the *data controller* or of a third party, and the processing for such purposes is proportionate to the restriction of the rights of the *data subject*.

Consent is deemed to be given: (i) in the case of the *data subject's* public appearance in respect of personal data disclosed or made public by him; or (ii) in the case of court proceedings or administrative proceedings commenced by the *data subject* in respect of personal data disclosed by him and required for conducting the proceedings. The consent can also be given in the framework of an agreement concluded with the *data subject*. No consent is required if the *data subject* cannot give his consent due to being legally incapacitated (e.g. physically or mentally disabled) or for another unavoidable reason and the processing is necessary to protect the vital interests of the *data subject* or other persons or to prevent a catastrophe or emergency.

The DPA contains exemptions for certain types of processing. For example, processing for private purposes is exempt from the scope of the DPA.

Are there any formalities to obtain consent to process personal data?

There are no formalities in relation to obtaining consent.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes: (i) the *standard types of sensitive personal data*; (ii) information about criminal records; and (iii) information about addictions.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may only be processed: (i) if the *data subject* has given his explicit consent in writing; (ii) if it is necessary for the enforcement of an international treaty or if an act of parliament prescribes it for the enforcement of a constitutional right or for national security or criminal law enforcement purposes in connection with sensitive data related to racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or ideological beliefs or interest group membership; or (iii) if prescribed by an act of parliament for public policy purposes in respect of other sensitive personal data.

There is specific legislation in relation to personal data processed for health and human genetics.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be explicit and given in writing.

Scope of Application

What is the territorial scope of application?

The DPA applies to all data management and data processing operations performed in the territory of Hungary, including the collection of personal data in Hungary. The DPA also applies if a *data controller* that processes data outside of the territory of the European Union: (i) engages a *data processor* that has its registered office, place of business, residence or domicile in Hungary; or (ii) uses technical equipment located in the territory of Hungary for its data processing activities, assuming that such equipment does not merely serve the purpose of data transfer through the territory of the European Union.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. The *data controller* shall be held responsible for the entire *data processing* activity, including the conduct of the *data processor* engaged by it.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to both manual and electronic records.

Rights of Data Subjects

Compensation

Data subjects can enforce their rights, and claim damages, directly in the courts which can, *inter alia*, lead to a public announcement about, or public apology in relation to, the breach.

Fair processing information

A *data controller* must provide *fair processing information* to *data subjects*. *Data subjects* must also be informed, *inter alia*, about the persons to whom data may be disclosed, their rights and remedies under the DPA and the duration of the data processing. Prior to the collection of data, the *data subject* must be informed whether disclosure is voluntary or compulsory and, in the latter case, on which basis.

If the provision of the above information to each individual *data subject* is impossible or would incur unreasonable expense, notifying the *data subject* (particularly for statistical or scientific purposes, including historical research) may be satisfied by publishing the following information: (i) the fact of the data collection; (ii) the scope of the *data subjects* involved; (iii) the purpose of the data collection; (iv) the duration of the proposed processing operation; (v) the data processing individuals authorised to access the data; (vi) the *data subjects'* rights and remedies related to the data processing; and (vii) the registration number of the respective data processing operation (if applicable).

Rights to access information

Data subjects may obtain their *subject access information* by request to *data controllers*. *Data subjects* are also entitled to the name and corporate address of any *data processor* engaged by the *data controller*. A subject access request is free of charge once a year; additional subject access requests require reimbursement of the *data controller's* costs. The fee is refundable if the data processing by the *data controller* proves to be illegal or the access request results in the rectification of the data.

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing data for direct marketing purposes.

Other rights

Any *data subject* may request the rectification or erasure of his personal data, with the exception of those processed by order of legal regulation. *Data controllers* must correct the data if they are false. Personal data must be erased if: (i) processed unlawfully; (ii) so requested by the *data subject*; (iii) deficient or inaccurate and cannot be legitimately corrected, provided that erasure is not disallowed by statutory provision; (iv) the purpose of processing no longer exists or the storage term defined by an act of parliament has expired; or (v) so ordered by the court or the Authority.

The *data subject* has the right, in line with the *Data Protection Directive*, to object to the processing of their data: (i) on compelling legitimate grounds relating to their particular situation to the processing of data relating to them, save where otherwise provided by law; (ii) if personal data are used or transferred for the purposes of direct marketing, public opinion polling or scientific research; and (iii) if the right to object is provided by law.

Security

Security requirements in order to protect personal data

Data controllers, and within their sphere of competence, *data processors*, must comply with the *general data security obligations*. For the technical protection of personal data, the *data controller*, *data processor* or operator of the telecommunications or information technology equipment shall implement security measures, in particular, if the processing involves the transmission of data over a network or any other means of information technology.

Specific rules governing processing by third party agents (processors)

The *data controller* must enter into a written contract for the processing of personal data. Any company interested in the business activity using the personal data may not be engaged for the processing of such data. Pursuant to the DPA, the *data processor* shall not be permitted to subcontract any part of its operations, i.e. it may not engage data sub-processors.

Notice of breach laws

The DPA does not contain any obligation to inform the Authority or *data subjects* of a security breach.

Specific notice of breach laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

According to the DPA, personal data (including sensitive data) may be transferred, irrespective of the medium and the manner in which it is transferred, to a *data controller* or *data processor* in a third country if: (i) the *data subject* has given his explicit consent; or (ii) the laws of the third country in question afford an adequate level of protection with respect to the processing of the data transferred.

An EU Commission finding on adequacy or a bilateral treaty or the use of *Model Contracts* all qualify as providing adequate protection within the meaning of the DPA. Hungary, as a member state of the European Union, is also bound by the Safe Harbor framework. The DPA currently does not provide for transfers of personal data to third countries pursuant to *binding corporate rules*.

Notification and approval of national regulator (including notification of use of Model Contracts)

It is not necessary to notify the Authority of the use of *Model Contracts*.

Use of binding corporate rules

The DPA currently does not provide for transfers of personal data to third countries pursuant to *binding corporate rules*. However, the Authority already recommended that the law should be amended to allow the use of *binding corporate rules*.

Enforcement

Sanctions

If the *data controller* or *data processor* fails to comply with the Authority's request to cease unlawful data processing, the Authority may order that unlawfully processed data be corrected, blocked, erased or destroyed, or the Authority may prohibit the unauthorised data management and/or processing operations and suspend any operation aimed at transferring data abroad. The Authority may order that the *data subject* be informed on any unlawful failure to comply with such a request.

Pursuant to the DPA, the Authority may also impose a regulatory fine of HUF 100,000 to HUF 10,000,000 (equivalent to approximately EUR 337 to EUR 33,700). The Authority may also announce its decision to the public.

Criminal sanctions apply in the case of serious breach of data protection regulations causing significant damage and include imprisonment of up to one year (three years in the case of sensitive data), public service or a fine of up to HUF 10,800,000 (i.e. approximately EUR 40,000). The *data subject* suffering the damage may also claim compensation in civil law proceedings.

Data controllers shall be liable for any damage caused to a *data subject* as a result of unlawful processing or by breaching the technical requirements of data protection. *Data subjects* may file for court action against the *data controller* for any violation of their rights. A *data controller* is relieved from liability if he proves that the occurring damage was caused by circumstances beyond his control. No compensation shall be paid where the damage was caused by intentional or negligent conduct on the part of the *data subject*.

Practice

Since the DPA established the new Authority and new procedural rules as of 1 January 2012, it is not yet possible to outline a general approach of such new Authority. However, there were a number of significant fines imposed on entities for breaching the previous data protection act.

Enforcement authority

As of 1 January 2012, the Authority acts as the enforcement authority with enhanced competencies. Criminal and civil courts are competent in criminal offences and civil law sanctions in connection with data protection.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Act No. C of 2003 on Electronic Communications (the "**Communications Act**"), and Act No. CVIII of 2001 (as amended by Act No. XCVII of 2003), in respect of certain aspects of electronic commerce services and information society services (the "**ECA**"), implemented Article 13 of the *Privacy and Electronic Communications Directive*. The ECA entered into force on 23 January 2002 and the Communications Act entered into force on 1 January 2004. Both the ECA and the Communications Act were amended several times during 2011 and 2012. Act No. XLVIII of 2008 on the Basic Conditions on and Restrictions of Commercial Advertising (the "**Advertising Act**") sets out the basic rules on direct marketing. The Advertising Act entered into force on 1 September 2008 and was also amended in 2011 and 2012.

The Communications Act was amended on 3 August 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The Communications Act does not expressly refer to the use of browser settings as a means to obtain consent. There is an express requirement for consent to be "prior" to the use of a cookie.

Regulatory guidance on the use of cookies

There is no specific regulatory guidance in respect of the use of cookies to date.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

According to the Advertising Act, direct marketing by e-mail is only authorised with the prior consent of the recipient.

Conditions for direct marketing by e-mail to corporate subscribers

It is not necessary to obtain consent to electronic advertising targeted at corporate subscribers. However, if the e-mail address contains personal data, the consent is only not required if it is clear that the *data subject* is a contact person of the entity concerned.

Exemptions and other issues

No exemptions apply.

The sender must include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The Communications Act requires that direct marketing messages through the telephone cannot be forwarded to subscribers who have opted out from the receipt of such messages. Notwithstanding this general position, there is a requirement for prior consent for direct marketing carried out to promote telecommunications services. In addition, customers have the right to indicate in the public directories that the published data cannot be used for marketing purposes.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The position is the same as for individual subscribers.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The Communications Act requires that direct marketing messages through the telephone cannot be forwarded to subscribers who have opted out from the receipt of such messages. Notwithstanding this general position, there is a requirement for prior consent for direct marketing carried out to promote telecommunications services. In addition, customers have the right to indicate in the public directories that the published data cannot be used for marketing purposes.

Conditions for direct marketing by fax to corporate subscribers

The position is the same as for individual subscribers.

Exemptions and other issues

No exemptions apply.

Iceland.

Contributed by LOGOS - Legal Services

General | Data Protection Laws

National Legislation

General data protection laws

The Act on the Protection of Privacy as regards the Processing of Personal Data No 77/2000 (the "**DPA**") implemented the *Data Protection Directive* into Icelandic law.

Entry into force

The DPA itself entered into force on 1 January 2001, but the amending Acts No 90/2001 and 81/2002, which implemented decisions of the EU Commission No 2000/518/EC, 2000/519/EC and 2000/520/EC, entered into force on 15 June 2001 and 17 May 2002, respectively.

National Regulatory Authority

Details of the competent national regulatory authority

The Data Protection Authority (the "**Authority**")
Rauðarárstíg 10
105 Reykjavík
Iceland

www.personuvernd.is

Notification or registration scheme and timing

Each *data controller* who uses electronic technology to process personal data must notify the Authority of the processing, using a form intended for that purpose, in a timely manner before beginning the processing. There are no notification costs. Any changes that are made after the original notification shall also be notified.

If the processing of general or sensitive personal data is likely to present specific risks to the rights and freedoms of *data subjects*, the Authority can decide that the processing may not begin until it has been examined by the Authority and approved of, by the issuing of a special permit. The Authority can decide that such permits will no longer be required when general rules and security standards, to be observed in this kind of processing, have been issued..

Exemptions

The Authority has issued instructions exempting: (i) data processing carried out in the ordinary course of business relating solely to those who have a connection to the activities or the relevant field of work; (ii) data processing necessary to fulfil legal obligations of the *data controller*; (iii) data processing necessary to fulfil a contract to which the *data subject* is a party, or an agreement between labour market organisations; (iv) data processing extending only to data that has been and is accessible to the public, provided that it is not aligned or combined with other personal data which has not been made accessible to the public; (v) data processing resulting from electronic surveillance, conducted for the purposes of security and property protection only, provided that legal obligations regarding notification have been fulfilled; (vi) wholly manual data processing; and (vii) data processing involving systematic recording of telephone calls.

These exemptions do not apply to electronic data processing of individual evaluations, aligning individuals to personal profiles or the transfer of unencrypted personal data abroad.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA is any data relating to a *data subject* who is identified or identifiable - i.e. information that can be traced directly or indirectly to a specific individual, deceased or living. The definition in the DPA is based on the *standard definition of personal data*.

The issue of whether information constitutes personal data is generally uncontroversial and normally it is clear whether it does fall within this definition. According to the Authority, IP addresses are generally considered to be personal data.

Is information about legal entities personal data?

In general, information about legal entities is not considered personal data. Sole traders and partnerships are, therefore, not treated as individuals under the DPA. However, some parts of the DPA have been extended to apply to both

individuals and legal entities. For example, Regulation on the Collection and Processing of Financial and Credit Standing Data No. 246/2001 was issued under the DPA and contains provisions that apply both to individuals and legal persons.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. The burden of proof of showing that processing conditions are satisfied is placed on the *data controller*.

The Authority can permit the processing of personal data in instances other than those above if it is considered to be either of urgent public interest or of individual interest, including the interest of the *data subject*.

Are there any formalities to obtain consent to process personal data?

In general, there are no formalities to obtain consent to process personal data under the DPA. The DPA does not require the consent of the *data subject* to be in writing unless the processing is for scientific research.

However, as the consent must be informed, the *data subject* must be given sufficient information regarding the processing of its personal data and an opportunity to object to it. The burden of proof is placed upon the *data controller* to show that this requirement is satisfied. Therefore, for evidential purposes, written consent is recommended in practice.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) information regarding whether the *data subject* has been suspected of, accused of, charged with or convicted of a criminal offence.

According to the Authority, the term "ethnic origin" does not apply to information regarding citizenship. The Authority also considers that biometric information can sometimes fall within the definition of sensitive personal data, particularly if the information reveals information regarding the health or origin of the *data subject*.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. Additional processing conditions are set out in the DPA and include processing necessary for: (i) the performance of a contract with the *data subject*; (ii) compliance with a legal obligation; (iii) the public interest or in the exercise of official authority; (iv) the *data controller's* legitimate interests, except where overridden by the interests of the *data subject*; (v) the *data controller* to carry out under contracts between the Social Partners; or (vi) the purposes of statistical or scientific research, provided that the privacy of individuals is protected by means of specific and adequate safeguards.

Material such as audio and video material, that is produced by means of electronic surveillance and includes sensitive personal data, may be collected even though the above requirements are not fulfilled, if the following conditions are met: (i) the surveillance is necessary and is conducted for the purposes of security and property protection; (ii) the material produced by the surveillance may not be disclosed to anyone else or processed further except (a) with the consent of the subject of the recording, (b) in accordance with a decision by the Authority, or (c) to the police if it contains data on accidents or a punishable legal offence; and (iii) the material that is collected in conjunction with the surveillance shall be deleted when there is no longer an apposite reason to preserve it, unless a special permit is issued by the Authority.

The Authority can permit the processing of sensitive personal data in instances other than those above if it considers it to be of urgent public interest. The Authority issues such permits on any conditions that it deems necessary in each case in order to protect the interests of the *data subjects*.

Are there any formalities to obtain consent to process sensitive personal data?

The position is the same as for personal data (see above). Again, written consent is recommended in practice.

Scope of Application

What is the territorial scope of application?

The DPA applies to the processing of personal data: (i) if it is conducted on behalf of a *data controller* established in Iceland, if the processing is carried out in the EEA, an EFTA country or a country or a place that the Authority lists in a notice in the *Law and Ministerial Gazette*; (ii) if the *data controller*, who is established in a country outside of the EEA or EFTA, makes use of equipment and facilities situated in Iceland; and (iii) about financial and credit standing data concerning legal persons using equipment in Iceland even if the *data controller* is not established in Iceland.

Points (ii) and (iii) do not apply if the equipment in question is only used to transmit personal data through the territory of Iceland. However, where points (ii) and (iii) do apply, the *data controller* must designate a representative established in Iceland, and the provisions of the DPA relating to *data controllers* shall then apply to that representative as fitting.

Who is subject to data protection legislation?

The DPA applies to *data controllers* and *data processors*.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to any electronic processing of personal data. It also applies to manual processing of personal data that form, or are intended to form, a part of a filing system. A filing system is any structured set of personal data where data on individual persons can be found.

Rights of Data Subjects

Compensation

If a *data controller* or a *data processor* has processed personal data in violation of the DPA or rules or instructions of the Authority, the *data controller* shall compensate the *data subject* for the financial damage suffered by him as a result of such violation. A *data controller* will, however, not be liable to pay compensation for any detriment he proves can neither be traced to his mistake nor to any negligence on his or his *data processor's* behalf.

Fair processing information

When a *data controller* obtains personal data from a *data subject*, the *data controller* is obliged to provide the *data subject* with the *fair processing information*. The information is not required in writing. The burden of proof, however, is placed upon the *data controller*. If the *data subject* insists upon receiving the information in writing, the *data controller* must comply.

The DPA also requires the provision of information about the recipients but does not specifically require the provision of information about the rights of the *data subject* (though this is good practice according to the Authority).

When a *data controller* collects personal data from someone other than the *data subject*, the *data controller* shall, with few exceptions, concurrently inform the *data subject* about the collection and other specific items listed in the DPA.

Finally, a *data controller* must also give a range of information about its processing to any person that requests such information.

There is no obligation in the DPA to provide this information in Icelandic, though it may be difficult to show that the information has been fairly provided if it is not in a language the *data subject* is familiar with. There is no obligation to refer to the DPA itself in any *fair processing information*.

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. The *data subject* also has a right to be informed by the *data controller* of: (i) his right to access/correct/delete the data; and (ii) the security measures in place, provided it does not diminish the security of the processing. There is generally no subject access request cost.

However, this right to information of the *data subject* does not apply if: (i) the data is used solely for statistical processing or scientific research and its processing cannot have direct influence on a *data subject's* interests; (ii) the rights of the *data subject*, under that clause, are deemed secondary, in part or wholly, to the interests of others or of his own; or (iii) the data is exempted from access under the Access to Information Act or the Administrative Procedures Act.

Objection to direct marketing

The *data subject* may require that the *data controller* stops processing data for direct marketing purposes. The *data controller* must then cease such processing immediately. The marketing restriction list operated by the national demographic registry is updated on a monthly basis.

Other rights

If incorrect, misleading or incomplete personal data has been registered, or if personal data has been registered without proper authorisation, the *data controller* shall rectify, erase, delete or correct such data to the extent the defect in question is liable to affect the interests of the *data subject*. If such data has been disclosed or used, then the *data controller* shall, to the extent that he is possibly able to, prevent it from affecting the interests of the *data subject*.

The *data subject* may object to the processing of personal data relating to him, save where otherwise provided by national legislation. In addition, the *data subject* has the right to be informed regarding electronic surveillance.

The *data subject* can ask about the reasons for individual decisions that are based on automated data processing. When personal profiles are used for specific purposes, the Authority can decide that the *data controller* shall notify the *data subject* and give him certain information.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations*. The *data controller* is responsible for establishing and updating risk analysis procedures and putting security measures in place, in conformity with laws, rules and instructions given by the Authority. The Authority has issued instructions which, amongst other things, recommend the use of encryption.

The *data controller* shall document the process by which he has produced a security policy, conducted a risk analysis and decided on security measures to be implemented. The Authority shall be granted access to this information on request.

Specific rules governing processing by third party agents (processors)

A *data controller* is permitted to use a *data processor* provided he: (i) has verified that the *data processor* in question will keep the information secure; and (ii) has the right to conduct an audit on the *data processor*.

The *data controller* must enter into a contract with the *data processor* in writing and at least in duplicate. The contract must in particular stipulate that the *data processor* shall act only on instructions from the *data controller* and that any processing by the *data processor* must comply with the DPA.

Anyone who acts in the name of the *data controller* or the *data processor*, including the *data processor* himself, and has access to personal data, may only process personal data according to the instructions of the *data controller*, unless legislative acts stipulate otherwise.

Notice of breach laws

The DPA does not contain any obligation to notify the Authority of a security breach. However, a notice is considered as good practice, particularly if the security breach is major. Moreover, *data controllers* in certain sectors may be required to inform sectorial regulators of any breach.

Specific notice of breach laws will apply to the electronic communications sector once the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive* have been implemented into national law.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the standard conditions for *transborder dataflow*. It has been recognised that the following countries provide an adequate level of protection of personal data (see Advertisement on Transborder Flows of Personal Data No 228/2010): the Member States of EES and EFTA; Switzerland; Canada; Argentina; Guernsey; the Isle of Man; Jersey; Faroe Islands; Andorra and Israel. The same applies if the transfer of data follows the principles of safe harbor and the Q&A issued by the U.S. Department of Trade, cf. Commission Decision 2000/520/EC of 26 July 2000. The *data controller* can rely on its own assessment of whether the personal data will be adequately protected after it has been transferred outside of the EEA.

The Authority can authorise the transfer of data to a country that does not provide an adequate level of personal data protection if: (i) the *data controller* has, in the opinion of the Authority, provided sufficient guarantees to protect such data; or (ii) the Authority determines that special circumstances warrant it, even if the *standard conditions for transborder dataflow* are not met. This requires the nature of the data, the planned purpose of the processing and its duration to be taken into account.

Notification and approval of national regulator (including notification of use of Model Contracts)

Transfer of personal data that is not encrypted is subject to notification. Otherwise there is no obligation to notify or obtain the consent of the Authority to any *transborder dataflows*; whether the transfer is to countries outside of the EEA or made in reliance on the *Model Contracts*.

Use of binding corporate rules

In practice, it may be necessary to adopt some form of *binding corporate rules* to satisfy the Authority that the personal data will be adequately protected once it is transferred outside of the EEA. The Authority follows a mutual recognition approach for the assessment of *binding corporate rules*.

Enforcement

Sanctions

Sanctions for breaching the DPA are both civil and criminal.

The Authority can order the cessation of processing of personal data, order the erasure of personal data, prohibit further use of data or instruct the *data controller* to implement measures that ensure the legitimacy of the processing.

Infringements of the provisions of the DPA, and of regulations issued under the DPA, are punishable by means of fines or a prison term of up to three years, unless more severe sanctions are provided for in other acts of law. The same punishment shall apply if instructions by the Authority are not observed. If an offence is committed as a part of the operations of a legal person, that legal person can be fined as provided for in Chapter II A of the General Penal Code.

Practice

In 2012, the Authority had 1,739 cases for inspection (at administrative level), of which 1,489 were new and 250 were continued from 2011. The last few years have seen a considerable increase in the number of new cases; there were 606 new cases in 2002, 676 in 2004, 764 in 2006, 904 in 2007, 985 in 2008, 1,156 in 2009, 1,221 in 2010 and 1,397 in 2011. The Authority has seen a 65% increase in the number of cases since 2007.

In 2012, 20 cases were initiated by the Authority, 459 cases were enquiries resulting in the issuing of opinions and 111 cases were complaints to which the Authority handed down its own decision.

The Authority does not refer cases to the police/prosecutor, as it is up to the person who thinks there has been an infringement of his privacy rights to make a complaint to the police. According to the Authority, two complaints have been made to the police, one at the end of 2010 and one in 2011. No complaint was made to the police in 2012. To date, no one has been prosecuted for infringements against the DPA. Since no prosecution has taken place and only the courts can impose penalties for infringements against the DPA, no penalties have been imposed.

Enforcement authority

The Authority has the power to impose daily fines of ISK 100,000, until it concludes that the necessary improvements have been made. If the Authority's decision to impose daily fines is referred to the courts, then the fines will not begin to accrue until a final judgment has been rendered. Daily fines are deposited in the State Treasury and may be collected by a distress action without prior judgment.

The Authority can assign to the Chief of Police the task of temporarily halting the operations of the party in question and sealing its place of operation without delay.

The Director of Public Prosecutions and the National Commissioner of the Icelandic Police have the power of prosecution.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Electronic Communication Act No 81/2003 (the "**ECA**"), which entered into force on 25 July 2003, implemented Article 13 of the *Privacy and Electronic Communications Directive*.

The ECA has not yet been amended to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. According to the Ministry of Interior the implementation of the *Citizens' Rights Directive* has currently been postponed and it has not been decided when the implementation will take place.

Cookies

Conditions for use of cookies

Currently, it is only necessary to inform users of the use of cookies and offer them the right to refuse their use. However, when the ECA is amended to implement the *Citizens' Rights Directive* it will be necessary to obtain consent to the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user.

Regulatory guidance on the use of cookies

As the ECA is being reconsidered, no regulatory guidance on the use of cookies is in place yet.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing by e-mail requires the prior consent of the recipient.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing by e-mail requires the prior consent of the recipient.

Exemptions and other issues

The *similar products and services exemption applies*. According to the ECA, the use of automated calling systems, facsimile machines or electronic mail for direct marketing is only allowed if a subscriber has given prior consent.

Further, unsolicited electronic communications in the form of direct marketing are not allowed to be sent to subscribers who do not wish to receive these communications.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to individual subscribers who have: (i) previously objected to such calls; or (ii) requested not to receive such direct marketing calls by a listing in the National Registry or the telephone directory.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to corporate subscribers who have either: (i) previously objected to such calls; or (ii) requested not to receive such direct marketing calls by a listing in the Company Registry or the telephone directory.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax is permitted so long as the recipient has not objected to receiving them.

Conditions for direct marketing by fax to corporate subscribers

Direct marketing by fax is permitted so long as the recipient has not objected to receiving them.

Exemptions and other issues

The *similar products and services exemption* applies. The name and address of the sender on whose behalf the communication is made must be clearly indicated in the fax.

India.

Contributed by Talwar Thakore & Associates

General | Data Protection Laws

National Legislation

General data protection laws

India is not a party to any convention on protection of personal data which is equivalent to the *Data Protection Directive*. However, India has adopted or is a party to other international declarations and conventions such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which recognise the right to privacy.

India has also not yet enacted specific legislation on data protection. However, the Indian legislature did amend the Information Technology Act (2000) ("**IT Act**") to include Section 43A and Section 72A, which give a right to compensation for improper disclosure of personal information.

The Indian central government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "**Rules**") under Section 43A of the IT Act. A clarification to the above Rules was issued on 24 August 2011 (the "**Clarification**"). The Rules have imposed additional requirements on commercial and business entities in India relating to the collection and disclosure of sensitive personal data or information which have some similarities with the *Data Protection Directive*.

Also relevant to the protection of personal data are indirect safeguards developed by the courts under common law, principles of equity and the law of breach of confidence and the following statutes: (i) Article 21 of the Constitution of India, which states that "no person shall be deprived of his life or personal liberty except according to procedure established by law". The Supreme Court of India has recognised the right to privacy under Article 21 of the Constitution as a part of the right to "life" and "personal liberty". However, this right to privacy is not an absolute right and is subject to overriding interests, including protection of health and freedom of information of others, national security and public morality; (ii) the Indian Penal Code 1860, which does not directly address breach of data privacy but has been used to bring prosecutions for data theft under Section 405 (criminal breach of trust), Section 406 (punishment for criminal breach of trust) and Section 420 (cheating and dishonestly inducing delivery of property).

Finally, the Credit Information Companies (Regulation) Act, 2005 ("**Act**") regulates a range of entities including credit information companies, credit institutions and other "specified users". This Act and rules and regulations made under it require the adoption of privacy "principles" for a wide range of activities relating to the use of credit information. However, this Act is not considered further in the summary below

Entry into force

Section 43A and Section 72A of the IT Act came into force on 27 October 2009.

The Rules came into force on 11 April 2011.

National Regulatory Authority

Details of the competent national regulatory authority

India does not have a national regulatory authority for protection of data.

The Ministry of Communications and Information Technology (the "**Ministry**") is responsible for administering the IT Act and issuing the Rules and other clarifications under the IT Act. The authorities established under the IT Act – i.e. the adjudicating officer and cyber appellate tribunal and, thereafter, the different High Courts and the Supreme Court, are responsible for enforcing the IT Act.

Ministry of Communications & Information Technology (Government of India)

Electronics Niketan, 6,
CGO Complex,
Lodhi Road,
New Delhi 110003

http://www.mit.gov.in/

Notification or registration scheme and timing

There is no requirement to register or provide prior written notification for processing data.

Exemptions

Not applicable.

Appointment of a data protection officer

Body corporates are required to designate a grievance officer who shall address any discrepancies or grievances of providers of information with respect to processing of information in a time-bound manner. The grievance officer is required to redress the grievance expeditiously, within one month from the date of receipt of such grievance. The body corporate is required to publish the name and contact details of the grievance officer on its website.

Personal Data

What is personal data?

Personal data under the Indian laws and rules is termed "**personal information**".

Personal information has been defined under the Rules as "any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person".

Is information about legal entities personal data?

No. Personal information pertains only to information about a natural person.

What are the rules for processing personal data?

There are no specific rules that govern the processing of personal data.

However, the Rules state that a body corporate or any person who processes personal information on behalf of the body corporate should provide a privacy policy. This privacy policy should serve to protect the personal information that is provided and the provider of such information should be able to review the policy. The privacy policy is required to be made available on the website of the body corporate and should provide for: (i) clear and accessible statements relating to its practices and policies; (ii) the type of personal information or sensitive personal data or information that is being collected; (iii) the purpose of collecting and using of such information; (iv) the instances in which disclosure of such information may be made under the Rules; and (v) reasonable security practices and procedures required under the Rules. A privacy policy is required even when no sensitive personal data or information is being processed.

Are there any formalities to obtain consent to process personal data?

No specific formalities for processing personal information have been stated. As per the Clarification, the Rules pertain only to collection, disclosure and transfer of sensitive personal data or information.

Sensitive Personal Data

What is sensitive personal data?

Sensitive personal data exists as the concept of sensitive personal data or information under the Rules. It means personal information which consists of: (i) passwords; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above items provided to a body corporate for providing services; and (viii) any of the information received under above items by a body corporate for processing, that is stored or processed under lawful contract or otherwise.

Sensitive personal data or information does not include information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005.

A "**provider of information**" is similar to a *data subject* and is defined as a natural person who provides sensitive personal data or information to a body corporate.

Are there additional rules for processing sensitive personal data?

The Rules contain specific provisions regarding the collection of sensitive personal data or information. They apply to all body corporates other than those providing services related to the processing of sensitive personal data or information to any person under a contract. However, such provisions will also apply to such exempted body corporates if they provide such services directly to the provider of information under a contract.

The key rules on collection are: (i) it is necessary to obtain the consent of the provider of information to the collection. The provider of information must be given an option not to provide the requested sensitive personal data or information and to withdraw its consent by informing the body corporate in writing; (ii) sensitive personal data or information can only be collected where necessary for a lawful purpose that is connected with a function or activity of the body corporate or any person on its behalf; (iii) the body corporate should provide additional information to the provider of information (see below); and (iv) the body corporate must comply with other general requirements, such as not keeping sensitive personal data or information for longer than is required and ensuring it is kept secure.

Additional rules apply to the disclosure of sensitive personal data and information. The body corporate and any person acting on its behalf are not allowed to publish any sensitive personal data or information. Further, the disclosure of

sensitive personal data or information to any third party requires the prior permission of the provider of information. The only two exceptions to this requirement are: (i) when such disclosure has been agreed upon in the contract between the body corporate and the provider of information; or (ii) when it is necessary to disclose the information in compliance with a legal obligation. The third party that receives such sensitive personal data or information shall not disclose it further and must be based in a country offering the same levels of data protection as India. The body corporate is allowed to share information with government agencies mandated under the law to obtain information.

Are there any formalities to obtain consent to process sensitive personal data?

Consent of the provider of information should be obtained in writing (which includes any mode of electronic communication) regarding the purpose of its usage and before further transfer or disclosure.

Scope of Application

What is the territorial scope of application?

The Rules issued under Section 43A of the IT Act apply only to a body corporate or any person located within India.

The provisions of the IT Act (except in respect of matters governed by the Rules) are also applicable to any offence committed by a person outside India using a computer, computer system or computer network located in India.

Who is subject to data protection legislation?

Indian law does not contain the concepts of *data controller* and *data processor*. Instead, the Rules refer to the concept of a body corporate. A body corporate is defined as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities".

Are both manual and electronic records subject to data protection legislation?

The Rules apply to both electronic and manual records of sensitive personal data or information.

Rights of Data Subjects

Compensation

Section 43A of the IT Act provides that bodies corporate possessing, dealing with or handling any sensitive personal data or information in a computer resource owned, controlled or operated by it would be liable to pay damages as compensation to affected persons if they are negligent in implementing and maintaining reasonable security practices and procedures to protect sensitive personal data or information.

Fair processing information

A body corporate collecting sensitive personal data or information should keep the provider of information informed about: (i) the fact that the information is being collected; (ii) the purpose for doing the same; (iii) the intended recipients; and (iv) the name and address of the agency collecting and retaining the information. All the requirements applicable to personal data, such as the requirement for a privacy policy (see What are the rules for processing personal data?), are applicable when processing sensitive personal data.

Rights to access information

A provider of information can access information provided by it upon request.

Objection to direct marketing

The IT Act and Rules do not impose any conditions regarding the usage of sensitive personal data or information for direct marketing. However, where the information is collected from a provider of information (i.e. in a situation in which sensitive personal data or information is collected), the prior consent of the provider of information must be obtained, including the purpose for which the information is being collected.

Other rights

The provider of information has the right to review the information provided. A body corporate cannot refuse such a request. Additionally, any discrepancies and inaccurate information can be corrected by the provider of information.

Security

Security requirements in order to protect personal data

The Rules provide that reasonable security practices and procedures need to be maintained by each body corporate. A body corporate or a person acting on its behalf is "considered to have complied with reasonable security practices and procedures if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business". The Ministry has listed the International Standard IS/ISO/IEC 27001 on "Information Technology - Security

Techniques - Information Security Management System -Requirements" as one such standard. Body corporates following other standards are required to get their security practice and standards notified to and approved by the Ministry for effective implementation.

A body corporate is required to have its security practice and procedures certified and audited by an independent auditor who is approved by the central government at least once every year.

Specific rules governing processing by third party agents (processors)

There are no specific rules that govern third party agents acting on behalf of a body corporate. They are governed by the same regime applicable to body corporates.

Notice of breach laws

There are no specific rules that deal with notices of breach.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The Rules provide that *transborder dataflows* of sensitive personal data or information can be made to any other body corporate or a person in India or located in any other country if the same levels of data protection in India are adhered to, provided that such transfer is necessary for the performance of a lawful contract between the body corporate or any person acting on its behalf and the provider of information or such transfer has been consented to by the provider of information.

There is no restriction under the Rules regarding *transborder dataflows* of information that is not sensitive personal data or information.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no additional requirement to notify or obtain the approval of any regulatory authority.

Use of binding corporate rules

Transborder dataflows are only allowed to jurisdictions that require body corporates situated there to provide the same level of data protection as in India. The data protection regime in India is bespoke in nature and may not be similar to the level of protection provided by *binding corporate rules*.

Enforcement

Sanctions

Section 43A of the IT Act provides that bodies corporate possessing, dealing with or handling any sensitive personal data or information in a computer resource owned, controlled or operated by it would be liable to pay damages as compensation to affected persons if they are negligent in implementing and maintaining reasonable security practices and procedures to protect sensitive personal data or information.

Additionally, Section 72A of the IT Act provides for a fine of up to INR 500,000 or imprisonment of up to three years or both when there is disclosure of personal information in breach of a lawful contract or without consent.

Practice

As the Rules have only come into effect recently, there is no significant court or regulatory practice on the application of their provisions.

Enforcement authority

In order to determine whether there has been a contravention of Section 43A or the Rules, the central government may appoint an adjudicating officer to hold an inquiry for this purpose. The adjudicating officer is required to have experience in the field of information technology and legal/judicial experience as prescribed by the central government. The adjudicating officer has jurisdiction over claims only up to a maximum of INR 50,000,000. Jurisdiction for all claims exceeding INR 50,000,000 is vested with the competent court. The orders of the adjudicating officer are appealable before the cyber appellate tribunal and, thereafter, to the High Courts and the Supreme Court. Otherwise, the data protection regime in India is enforced by the courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Apart from the Telecom Commercial Communications Customer Preference Regulations, 2010 ("**Customer Preference Regulations**") issued by the Telephone Regulatory Authority of India ("**TRAI**") to telecom service providers to set up a mechanism to register requests of subscribers not to receive unsolicited commercial calls, there are no specific laws or regulations in India on the use of cookies or direct marketing.

Cookies

Conditions for use of cookies

There are no specific laws or regulations in India on the use of cookies.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

There are no specific laws or regulations in India on direct marketing by email.

Conditions for direct marketing by e-mail to corporate subscribers

Not applicable.

Exemptions and other issues

Not applicable.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to send unsolicited commercial communication by message, voice or SMS to individual subscribers who are listed in the 'fully blocked category' of the National Customer Preference Register established under the Customer Preference Regulations.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

There are no separate rules for corporate subscribers, who are governed by the same regime as non-corporate subscribers.

Exemptions and other issues

The NCPR provides customers the option to register under the 'partially blocked category' pursuant to which customers can opt for receiving promotional communications under the following categories: (i) banking/insurance/financial products/credit cards; (ii) real estate; (iii) education; (iv) health; (v) consumer goods and automobiles; (vi) communication/broadcasting/entertainment/IT; and (vii) tourism and leisure.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

There are no specific laws or regulations in India on direct marketing by fax.

Conditions for direct marketing by fax to corporate subscribers

Not applicable.

Exemptions and other issues

Not applicable.

Indonesia.

Contributed by Widyawan & Partners

General | Data Protection Laws

National Legislation

General data protection laws

There is no consolidated data protection law in Indonesia. However, there are a number of laws that address data protection issues. These laws are: (i) Law No. 11 of 2008 on Electronic Information and Transaction ("EIT Law"); (ii) Government Regulation No. 82 of 2012 on Implementation of System and Electronic Transactions ("GR 82"); (iii) Law No. 39 of 1999 on Human Rights ("**Human Rights Law**"); (iv) Law No. 8 of 1999 on Consumer Protection; (v) Indonesian Criminal Code; and (vi) Indonesian Civil Code.

The EIT Law and GR 82, the two key laws regulating data protection in Indonesia, apply to data held electronically. There are also other industry-specific laws and regulations that regulate data protection in particular industries, for example, the banking and health sectors. This summary does not address these industry-specific laws and regulations.

Entry into force

The EIT Law came into force on 21 April 2008. GR 82 came into force on 15 October 2012. The Human Rights Law came into force on 23 September 1999. Law No. 8 of 1999 on Consumer Protection came into force on 20 April 2000. The Indonesian Criminal Code came into force on 1 January 1918. The Indonesian Civil Code came into force on 30 April 1847.

National Regulatory Authority

Details of the competent national regulatory authority

The data protections laws are mainly enforced by the Ministry of Communication and Information ("**Menkominfo**").

Jl. Medan Merdeka Barat No. 17, Jakarta 10110, Indonesia

www.kominfo.go.id

Notification or registration scheme and timing

There is no notification or registration scheme.

Exemptions

Not applicable.

Appointment of a data protection officer

There is no requirement in the EIT Law or GR 82 to appoint a data protection officer. However, there is a general requirement under GR 82 that the electronic system operator (as defined below) must appoint a certified expert in the fields of electronic systems and information technology. The term "electronic system operator" is defined to mean any person, state official, business entity or society that provides, manages and/or operates, jointly or singly, an electronic system for the users of the electronic system for the operator's interest and/or others.

Personal Data

What is personal data?

Article 1.27 of GR 82 defines personal data as the data of individuals that is stored and maintained, the truthfulness of which is maintained and the secrecy of which is protected. This differs from the *standard definition of personal data*.

Is information about legal entities personal data?

Yes. Under GR 82 legal entities are *data subjects*.

What are the rules for processing personal data?

Under the EIT Law, unless exempted under other applicable laws or regulations, the prior consent of the *data subject* must be obtained in order to process their personal data in an electronic system. Although not specifically required, it is good practice to explain the practices for data use, processing, transfer and disclosure in detail in the consent document.

Are there any formalities to obtain consent to process personal data?

No. Online or electronic consents (such as clicking an 'agree' button provided with a consent notice) constitute valid legal evidence under the EIT Law. However, the courts might not accept such evidence and it is therefore recommended to obtain the *data subject's* express consent in writing for evidentiary purposes.

Sensitive Personal Data

What is sensitive personal data?

The EIT Law and GR 82 do not specifically distinguish between sensitive and non-sensitive personal data.

Are there additional rules for processing sensitive personal data?

No.

Are there any formalities to obtain consent to process sensitive personal data?

No.

Scope of Application

What is the territorial scope of application?

Article 2 of the EIT Law provides that the EIT Law applies to a "legal act" (this term is not defined) of any person (whether an individual or legal entity) inside or outside the territory of the Republic of Indonesia, which has legal effect inside or outside the territory of the Republic of Indonesia and which is "detrimental to the interest of the Republic of Indonesia". The law applies to legal acts performed not only in Indonesia or by Indonesian citizens, but also outside the jurisdiction of Indonesia by both Indonesian and foreign citizens or legal entities.

A legal act is "detrimental to the interest of the Republic of Indonesia" if, among other things, it is detrimental to the interests of the national economy, strategic data protection, the nation's dignity and degree, state defence and security, sovereignty, citizens or Indonesian legal entities.

Who is subject to data protection legislation?

The EIT Law applies to any person performing a legal act which is detrimental to the interest of the Republic of Indonesia (see above) and applies to both individuals and legal entities.

The EIT Law does not distinguish between: (i) entities which 'control', as opposed to 'process' personal data; (ii) recipients or senders of data; or (iii) business and non-business data.

Are both manual and electronic records subject to data protection legislation?

The EIT Law and GR 82 apply to data held electronically and hard copy print outs of electronic data. The Indonesian Criminal Code, the Indonesian Civil Code and the Human Rights Law apply to hard copy records that are not held electronically.

Rights of Data Subjects

Compensation

Data subjects have the right to compensation for contravention of their rights under the EIT Law and GR 82. These laws entitle a *data subject* to claim damages for loss against any party which causes that loss. Further, any breach of confidentiality or use of personal data by the electronic system operator contrary to the EIT Law or GR 82 is subject to administrative sanctions (including penalties).

In addition, compensation may be available under the Indonesian Civil Code. This is based on the general law of tort under Article 1365 of the Indonesian Civil Code and allows an aggrieved *data subject* to claim damages for actual loss suffered by the *data subject* where that loss is caused by an unlawful act of an electronic system operator. In this context, the term "unlawful act" is interpreted broadly, including not only violations of statutory law, but also violations of public morals or the duty of care owed to other persons' interests. There is no clear definition in Indonesian law on what violates "public morals" or "duty of care". The meaning of these terms varies over time and in different places.

Fair processing information

There is no specific requirement to inform the *data subjects* of how their personal data will be used. However, it is good practice to inform *data subjects* of how their personal data will be used or processed as part of the process of obtaining consent.

Rights to access information

Yes. *Data subjects* have a right to review personal data held by electronic system operators about them, based on the elucidation of Article 26.1 of the EIT Law (an elucidation constitutes part of the law and has legal effect under Indonesian law). Although not specifically required, it is good practice to outline the manner in which access may be obtained in the consent document provided to the *data subject*.

Objection to direct marketing

There are no specific provisions regarding the right to object to direct marketing. However, it is good practice to inform *data subjects* if their personal data will be used for direct marketing as part of the process of obtaining consent.

Other rights

No other specific rights are granted to *data subjects*. However, if a recipient of data grants *data subjects* other rights in relation to their personal data, for example, a right to request correction of personal data, it is good practice to inform *data subjects* of such other rights as part of the process of obtaining consent.

Security

Security requirements in order to protect personal data

GR 82 imposes a general requirement on the electronic system operator to implement a security system to protect personal data. These requirements are substantially the same as the *general data security obligations*.

Specific rules governing processing by third party agents (processors)

There are no specific rules relating to processing by third party agents. However, if an electronic system operator engages a third party agent, it is good practice to inform *data subjects* that their personal data will be accessed and processed by a third party agent and obtain their consent to this.

Notice of breach laws

Yes. An electronic system operator is required under the EIT Law and GR 82 to notify the *data subject* if the electronic system operator's security system has been breached.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

There are no specific provisions restricting the transfer of personal data to third countries. However, an electronic system operator for public services is required to build its data centre in Indonesia. The term "public services" is broadly defined under Law No. 25 of 2009 on Public Services ("**Law 25**") and includes the provision of goods, services, and administrative services provided by government institutions or state-owned enterprises. Under the elucidation of Article 5.7(b) of Law 25, public services extend to the provision of administrative services, such as issuing documents like payment receipts, by non-government institutions in the fields of banking, insurance, health, security, industrial services and social activities. In respect of such services in those fields, non-government institutions must build a data centre in Indonesia. However, this requirement does not usually extend to the day-to-day activities of those entities, as relevant administrative services are only those which are mandated by the government, based on applicable laws and regulations and implemented pursuant to an agreement with the services recipient.

In addition, an electronic system operator must store transactional data in Indonesia. The requirement to store data arising from electronic transactions between electronic system providers and their customers in Indonesia applies to both private and public electronic system providers under GR 82. There is no definition of "transactional data" in this context. However, it is likely to be limited to specific information in relation to the transaction itself (for example, the parties' identities and the purpose and value of the transaction).

Notification and approval of national regulator (including notification of use of Model Contracts)

There are no general provisions requiring notification or consent by a regulator for transfer of personal data to third countries, but industry-specific laws and regulations (for example, in the banking sector) may contain requirements to notify or obtain consent from a national regulator in certain circumstances.

Use of binding corporate rules

There is currently no ability to use *binding corporate rules* under the EIT Law or GR 82.

Enforcement

Sanctions

Breaches of the EIT Law may lead to administrative and civil liability, as well as certain criminal sanctions for violations of privacy, which include fines (ranging from IDR 1 billion to IDR 12 billion (approximately EUR 77,000 to EUR 923,000) and/or between one and twelve years imprisonment.

Practice

We are not aware of any significant court cases directly relating to the unlawful use or processing of personal data.

Enforcement authority

Menkominfo and the police are authorised to investigate any breaches of the EIT Law. While sanctions are determined by the courts, Menkominfo may impose administrative sanctions in accordance with GR 82.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

There are no specific ePrivacy laws, and the EIT Law and GR 82 do not contain provisions on direct marketing. However, any marketing materials distributed to consumers in Indonesia should be compliant with applicable Indonesian consumer protection laws (including the specific consumer protection provisions of the EIT Law and the general requirements under Law No. 8 of 1999 on Consumer Protection).

Cookies

Conditions for use of cookies

The use of cookies is not specifically regulated in Indonesia.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under the EIT Law, personal data processing is only allowed with the prior consent of the *data subject*. In practice, senders of direct marketing by e-mail use the following process to comply with the EIT Law: (i) send an email which identifies the sender and explains the purpose of the e-mail to the recipient; and (ii) stop sending direct marketing by e-mail to the recipient if the recipient does not reply to the first e-mail.

Conditions for direct marketing by e-mail to corporate subscribers

There are no specific provisions on the conditions for sending direct marketing by e-mail to corporate subscribers. However, the provisions applying to individuals described above also apply to corporate subscribers.

Exemptions and other issues

Not applicable.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Under the EIT Law, personal data processing is only allowed with the prior consent of the *data subject*. In practice, telephone marketers use the following process to comply with the EIT Law: (i) place a call which identifies the caller and explains the purpose of the call to the recipient; and (ii) stop the call if the recipient does not wish to continue the call.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

There are no specific provisions on the conditions for sending direct marketing by telephone to corporate subscribers. However, the provisions applying to individuals described above also apply to corporate subscribers.

Exemptions and other issues

Not applicable.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Under the EIT Law, personal data processing is only allowed with the prior consent of the *data subject*. In practice, senders of direct marketing by fax use the following process to comply with the EIT Law: (i) send a fax which identifies the sender and explains the purpose of the fax to the recipient; and (ii) stop sending direct marketing by fax to the recipient if the recipient does not contact the sender after receiving the first fax.

Conditions for direct marketing by fax to corporate subscribers

There are no specific provisions on the conditions for sending direct marketing by fax to corporate subscribers. However, the provisions applying to individuals described above also apply to corporate subscribers.

Exemptions and other issues

Not applicable.

Ireland.

Contributed by Mason Hayes + Curran

General | Data Protection Laws

National Legislation

General data protection laws

The Data Protection Act 1988 (the "**1988 Act**"), as modified by the Data Protection (Amendment) Act 2003 (the "**2003 Act**") (collectively, the "**DPA**") transpose the *Data Protection Directive* (Directive 95/46/EC) into Irish law. Irish law is supplemented by secondary legislation in the form of statutory instruments.

Entry into force

Most of the implementing provisions came into force on 1 July 2003. One provision of the 2003 Act prohibiting forced *data subject* access requests in the context of employment applications has yet to come into force.

National Regulatory Authority

Details of the competent national regulatory authority

Office of the Data Protection Commissioner (the "**DPC**")
Canal House
Station Road
Portarlington
Co. Laois
Ireland

www.dataprotection.ie

Notification or registration scheme and timing

While under the 2003 Act all *data controllers* and *data processors* are required to register with the DPC, the Irish registration regime contains wide exemptions for certain categories of processing that do not trigger a registration obligation. There are also certain categories of *data controller* that are subject to an absolute obligation to register.

Data controllers and/or *data processors* are obliged to renew their registration annually. The DPC may refuse an application for registration under certain conditions. There is a right of appeal against a refusal to the Circuit Court.

Registration costs EUR 480 (EUR 430 for an online application) for applicants with more than 25 employees, EUR 100 (EUR 90 for an online application) for applicants with between 6 and 25 employees and EUR 40 (EUR 35 for an online application) in all other cases.

Exemptions

The 2003 Act exempts: (i) not for profit organisations; and (ii) *data controllers* and *data processors* that process personal data in a public register or who only process manual data.

The Data Protection Act 1988 (Section 16(1)) Regulations, 2007 (the "**2007 Regulations**") exempt: (i) *data controllers* that only process employees' human resources data; (ii) candidates for political office and elected representatives; (iii) schools, colleges, universities and similar educational institutions; (iv) solicitors and barristers; (v) *data controllers* who process customer and supplier data in the context of normal commercial activity; (vi) companies who process personal data of past and present shareholders, directors or other officers in complying with the Irish Companies Acts; (vii) *data controllers* who process personal data for the purpose of publishing journalistic, literary or artistic material; and (viii) *data controllers* or *data processors* who operate under a data protection code of practice. *Data processors* that process personal data on behalf of any of the above categories of *data controller* are also not required to register.

However, the 2007 Regulations impose an absolute obligation to register on banks, insurance undertakings, direct marketing firms, debt collection agencies, credit reference agencies, health professionals, anyone processing genetic data, ISPs and telecoms companies. Any *data processor* that processes personal data on behalf of a *data controller* that falls into one of these categories is also obliged to register.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer. However, the DPC recommends that *data controllers* appoint a co-ordinator to deal with subject access requests. Where a data protection officer is appointed, this information should be supplied to the *data subjects*. A nominated contact for subject access requests also needs to be provided when making a registration application.

Personal Data

What is personal data?

The DPA only applies to personal data, defined as "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the *data controller*". This definition is therefore closely based on the *standard definition of personal data*. The DPC has endorsed the *Opinion on Personal Data*.

The High Court of Ireland considered the definition of personal data under the DPA in *EMI & others v Eircom Limited* [2010] IEHC 108 where it held on the facts that IP addresses did not comprise personal data. This decision may, however, be inconsistent with the position subsequently adopted the Court of Justice of the European Union in *Scarlet v. SABAM* [2011] ECECJ C-70/10.

Is information about legal entities personal data?

No. The DPA only applies to living individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. While consent is relied upon as a processing condition in many cases, *data controllers* often invoke the legitimate interest condition.

Are there any formalities to obtain consent to process personal data?

There are no formalities under the DPA to obtain consent to process personal data. Consent can be express, written or implied. Following the position of the Article 29 Working Party, the DPC may consider that consent from an employee is not freely-given consent and may be insufficient to legitimise the processing of personal data of employees in an employment context.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) information about criminal offences or criminal proceedings.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. Additional legitimate processing conditions are set out in the 2003 Act. These include processing for statistical purposes, political activities, the collection of taxes, assessment of entitlement to social welfare benefits and processing that is authorised by regulations made by the Minister for Justice for reasons of substantial public interest.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be explicit, may be given orally or in writing, and must be obtained before a *data controller* can process sensitive personal data. It would be insufficient to ask a *data subject* to indicate if he or she objects to such sensitive data being processed.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

Most obligations under the DPA are imposed on *data controllers*. However, *data processors* are required to have appropriate security measures in place in respect of the personal data they process. *Data processors* also owe a duty of care to *data subjects*.

Are both manual and electronic records subject to data protection legislation?

For the purposes of the DPA, data means information in a form in which it can be processed and this includes both manual and electronic records. However, only those manual records that are stored in a structured filing system are covered by the DPA.

Rights of Data Subjects

Compensation

The DPA also imposes a duty of care on *data controllers* and *data processors* towards *data subjects* in respect of the collection of their personal data and their dealings with that data. Therefore, in the event of a breach of the DPA by a *data*

controller or *data processor*, a *data subject* might be in a position to make a claim for damages against that *data controller* or *data processor* for breach of its duty of care towards the *data subject*.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. A *data controller* is obliged to explain the *fair processing information* to *data subjects*.

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. There are a number of prescribed exceptions to this right. An application must be in writing and a statutory fee of EUR 6.35 may be payable. Requests must be processed within 40 days.

Objection to direct marketing

Where personal data are kept for the purposes of direct marketing, Section 2(7) of the DPA provides that where the relevant *data subject* requests in writing that the *data controller* in question cease processing the data for that purpose, then generally, the *data controller* has 40 days to accede to such a request.

Other rights

An individual may apply to a *data controller* who keeps personal data relating to him to have data rectified, blocked or erased in case of contravention of the data protection principles.

A *data subject* may, in certain instances, request a *data controller* ceases processing his data for a specified purpose or in a specified manner.

Security

Security requirements in order to protect personal data

Data controllers and *data processors* must comply with the *general data security obligations*.

Specific rules governing processing by third party agents (processors)

Where processing of personal data is carried out by a *data processor*, the *data controller* must ensure that the processing is carried out in pursuance of a contract in writing or equivalent that contains the *standard processor obligations*.

Notice of breach laws

No explicit breach notification obligation is imposed on *data controllers* or *data processors* under the DPA. However, in July 2010, the DPC approved and published a *Personal Data Security Breach Code* which has wide ranging implications for organisations who suffer a data security breach. The Code introduces a disclosure regime which obliges organisations to contact the DPC where they suffer a security breach except in some limited circumstances. Organisations may also need to contact *data subjects* whose data is compromised by a security breach. Previously, any such notifications, whether to the DPC or affected individuals, would have been on a voluntary basis only. At present, the Code does not have the force of law, but it is expected to become binding quite soon.

Specific notice of breach laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

During 2011, the DPC received 1167 data security breach notifications from 186 different organisations. This represents a sharp increase on the 410 notifications received by the DPC in 2011.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the *standard conditions for transborder dataflow* and where the transfer is required under any enactment or required by any convention or instrument imposing an international obligation on the Irish State. The DPC has issued guidance in relation to when the prescribed exceptions may be relied upon. Following the Article 29 Working Party position, his view is that *data controllers* should be extremely cautious about relying on consent as a basis for data transfers since such consent needs to be clear, unambiguous, freely given and specific, which can be difficult to demonstrate in practice. Instead he recommends that other exceptions such as *Model Contracts* be relied upon.

Notification and approval of national regulator (including notification of use of Model Contracts)

Provided *Model Contracts* are used, without material amendments being made to them, there is no requirement to provide such contracts to the DPC for approval. If a *data controller* wishes to rely on *binding corporate rules*, then it may need to notify the DPC where its headquarters or main EU centre of activity is in Ireland.

Use of binding corporate rules

The DPC recognises the use of *binding corporate rules*, and has agreed to follow the mutual recognition process. However, most Irish *data controllers* tend to rely on one of the other prescribed exceptions. The DPC will need to approve any proposed *binding corporate rules*, as mere notification is insufficient. The DPC acted as the lead authority for the approval, in January 2012, of Intel's *binding corporate rules*.

Enforcement

Sanctions

A breach of a data protection principle is not of itself a criminal offence, but may result in an enforcement notice being issued by the DPC (see the section entitled "**Enforcement authority**" below). Failure to comply with an enforcement notice can constitute an offence punishable by fines up to EUR 100,000 on indictment but not prison sentences.

Any failure by a *data controller* or processor to register, where required to do so, is an offence punishable by a fine of up to EUR 100,000. Additionally, the unauthorised disclosure of personal data by a *data processor* is an offence, also attracting a maximum fine of EUR 100,000.

Practice

In 2011, the DPC opened 1,161 complaints for investigation. This represents a sharp increase on the 783 complaints filed in 2010.

Complaints concerning access rights accounted for approximately 48% of the overall total.

Most complaints were resolved informally without the DPC being required to make a formal decision under the DPA.

The DPC frequently issues guidance notes which seek to confer clarity on a number of different data protection issues. The guidance notes are available at www.dataprotection.ie.

Enforcement authority

The DPC may launch investigations into possible contraventions of the legislation and has the power to seek an amicable resolution or issue a decision. The DPC has no power to issue fines in respect of contraventions. However, the DPC in exercising its investigation powers may issue an enforcement notice which is subject to a right of appeal by either party to the courts. Prosecutions for criminal offences may be brought by the DPC before the Irish courts, who may then impose fines.

The DPC has the power to conduct comprehensive privacy audits of *data controllers*, as the DPC thinks fit, in order to ensure compliance with the DPA. Such audits are supplementary to investigations carried out in response to specific complaints. In 2011, twenty-eight privacy audits of *data controllers* were carried out by the DPC.

The DPC may also issue a prohibition notice in order to prohibit the transfer of personal data from Ireland to a country or territory outside of the EEA. Such a notice may prohibit the transfer concerned absolutely or until the *data controller*/*data processor* concerned has taken such steps as are specified in the notice for protecting the interests of the *data subjects* concerned. The *data controller*/*data processor* may appeal to the court against the prohibition in the notice within 21 days of service. It is an offence to refuse or fail to comply with a prohibition specified in the notice.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the "**2011 Regulations**") implemented Article 13 of the *Privacy and Electronic Communications Directive* as amended by the *Citizens' Rights Directive*. These regulations came into effect on 1 July 2011. One can be indicted under the 2011 Regulations for sending unsolicited communications. The penalty for a body corporate on conviction on indictment can be up to EUR 250,000. Where the person tried on indictment is a natural person, the fine imposed may not exceed EUR 50,000.

Cookies

Conditions for use of cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The 2011 Regulations expressly refer to the use of browser settings as a means to obtain consent. There is no express requirement for consent to be "prior" to the use of a cookie.

Regulatory guidance on the use of cookies

The DPC has provided regulatory guidance on the use of cookies which can be accessed at http://www.dataprotection.ie/documents/guidance/Electronic_Communications_Guidance.pdf.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The prior consent of subscribers is required before marketing to those individuals by e-mail.

Conditions for direct marketing by e-mail to corporate subscribers

The sending of unsolicited e-mail to corporate subscribers for the purpose of direct marketing is permitted unless the subscriber has informed the sender that it does not consent to the receipt of such messages.

Exemptions and other issues

It is permitted to use a customer's e-mail contact details if the *similar products and services exemption* applies. The 2011 Regulations also prohibit direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing calls may be made to an individual subscriber provided the subscriber has not previously objected to receiving such calls or noted his preference not to receive direct marketing calls in the National Directory Database.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Direct marketing calls may be made to a corporate subscriber provided the corporate subscriber has not previously objected to receiving such calls. It is not permitted to make direct marketing calls to a corporate subscriber if that corporate subscriber has noted a preference not to receive direct marketing calls in the National Directory Database.

Exemptions and other issues

No exemptions apply.

Direct marketing calls cannot be made to a mobile telephone in the absence of prior consent.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send a direct marketing fax to the telephone line of an individual subscriber unless that subscriber has previously consented to receiving such a fax.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send a direct marketing fax to the telephone line of a corporate subscriber if that subscriber has previously instructed the sender that it does not wish to receive such communications or has recorded a general opt-out to receiving such direct marketing faxes in the National Directory Database.

Exemptions and other issues

No exemptions apply.

Israel.

Contributed by Tene & Associates

General | Data Protection Laws

National Legislation

General data protection laws

Privacy is a constitutional right under Article 7 of Basic Law: Human Dignity and Liberty.

In addition, the Privacy Protection Act, 5741-1981 ("**PPA**"), contains specific privacy legislation. Chapter B of the PPA deals with data protection.

Entry into force

The PPA entered into force in 1981.

National Regulatory Authority

Details of the competent national regulatory authority

The Israeli Law, Information and Technology Authority ("**ILITA**")
125 Begin Road
P.O. Box 7360
Tel Aviv 61072

http://www.justice.gov.il/MOJEng/ILITA/

Notification or registration scheme and timing

Under the PPA a "database" must be registered with the Database Registrar, a unit of ILITA, if it contains: (i) data concerning more than 10,000 *data subjects*; (ii) sensitive information; (iii) data which have been collected from third parties; (iv) data used for direct marketing services; or (v) data in a public sector database. The term "database" refers to a collection of data processed by computer but excludes information consisting solely of basic contact details if such details are not in themselves likely to infringe an individual's privacy.

The registration system is based on registration of databases, as opposed to *data controllers*. Hence, if a *data controller* has several databases, such as human resources, customer data, and suppliers, it must register each database separately.

There is no requirement to obtain authorisation from the Database Registrar.

A January 2007 report of a Ministry of Justice committee (the "**Schoffman Report**") recommended that database registration obligations should be significantly narrowed. Although these recommendations were embraced by ILITA, they have yet to become law. In 2012, the Israeli Ministry of Justice circulated a draft bill for replacing most database registration obligations with internal documentation and accountability requirements. The draft bill is yet to become a formal government sponsored legislative proposal.

Exemptions

Only databases meeting the conditions set out above must be registered. However, given the broad definition of the term "sensitive data", most businesses are required to register at least one database.

Appointment of a data protection officer

No. However, each database must have a "database manager", who by default is the company's CEO, unless he/she appoints an officer for that role.

In addition, public sector entities, financial sector entities, and companies holding five or more databases subject to mandatory registration must appoint a chief information security officer.

Personal Data

What is personal data?

The equivalent term to "personal data" is "information", defined in Section 7 of the PPA as "details concerning an individual's personality, personal status, intimate relations, health condition, financial condition, vocational qualifications, opinions and religious belief".

The Israeli Supreme Court interpreted the term broadly to include information about an identifiable, though unidentified individual, such as an IP address (Civ. App. 4447/07 Rami Mor v. Barak ETC (Sup. Ct., 25 March 2010)); as well as details apparently not covered by the Section 7 definition, such as a person's address and telephone number, bank account information and national ID number (Civ. App. 439/88 Database Registrar v. Ventura, 48(3) P.D. 808 (1994)).

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

The PPA generally requires *data subject* consent for any processing. Such consent may, however, be implied. In addition, the PPA permits the processing of personal data under a legal obligation.

Additional rules applying to processing personal data are transparency; purpose limitation; *data subject* access, correction and rectification rights; data security and confidentiality.

Over the past two years, ILITA has issued guidance documents and market instructions concerning issues such as data processing in the context of outsourcing; requirements for user authentication when providing remote access to personal data; CCTV; smart cards in public transportation; employee screening and employment recruitment agencies; and the allocation of responsibility for databases between health insurers and primary health care providers. In addition, ILITA issued a draft instruction concerning the collection of data from minors and draft guidance concerning privacy in the workplace.

Are there any formalities to obtain consent to process personal data?

Consent means "informed consent, express or implied". There are no formalities to obtain consent.

Sensitive Personal Data

What is sensitive personal data?

The term "sensitive information" is defined broadly under Section 7 of the PPA to include "details concerning an individual's personality, intimate relations, health condition, financial condition, opinions and religious belief".

This definition is effectively identical to the term "information" except for two categories: "personal status" and "vocational qualifications", which appear only in the definition of the latter term.

Are there additional rules for processing sensitive personal data?

Under the Privacy Protection Regulations (Conditions for Data Storage and Security and Public Sector Data Sharing), 1986 (the "**Security Regulations**"), stricter data confidentiality and security requirements apply to certain categories of sensitive information, including health data and information concerning intimate relations ("**Limited Data**").

In addition, any database containing "sensitive information" is subject to mandatory registration under the PPA.

Are there any formalities to obtain consent to process sensitive personal data?

Consent means "informed consent, express or implied". There are no formalities to obtain consent.

Scope of Application

What is the territorial scope of application?

There is no provision on applicable law in the PPA, so the territorial scope of the statute needs to be determined according to general principles of choice of law. It is likely that the PPA will apply to: (i) controllers based in Israel; (ii) data processing operations in Israel; and (iii) the processing of personal data with respect to Israeli citizens, regardless of where such processing takes place.

Who is subject to data protection legislation?

The PPA uses the term "database owner" which is not defined in the PPA but is generally considered to be equivalent to the concept of *data controller*.

The PPA also uses the term "possessor" of a database which means "a person who has a database in his possession permanently and is permitted to use it". This is generally considered to be equivalent to the concept of *data processor*.

The distinction between a "database owner" and "possessor", much like that between *data controller* and *data processor*, is made for the purpose of allocation of responsibility. Most obligations under the PPA, including registration, notice, purpose limitation, access and rectification, security, and right of objection to direct marketing, apply to the "database owner". In addition, the "database owner" is the party against whom *data subjects* are entitled to exercise their rights. The "possessor" is subject to only confidentiality and security requirements.

The PPA also uses the term "database manager" to mean "an active manager of a body that owns or possesses a database or a person whom the aforesaid manager authorized for this purpose."

Are both manual and electronic records subject to data protection legislation?

Chapter B of the PPA only covers electronic databases, not manual ones. This accounts for the EU adequacy decision's restricted scope (see below). However, personal data in manual records is protected by Chapter A of the PPA, which specifies the principles of purpose limitation, confidentiality, transparency and informed consent.

As a result of this distinction, the European Commission's approval of Israel as a country providing "adequate protection" for personal data is restricted to: (i) automated international data transfers from the EU; and (ii) non-automated data transfers that are subject to further automated processing in Israel.

Rights of Data Subjects

Compensation

A violation of Chapter B of the PPA is a civil tort, creating for individuals a private cause of action. An individual whose rights are infringed not only under Chapter B but also under the general provisions of Chapter A of the PPA may be entitled to statutory damages in an amount up to NIS 50,000 (10,000 Euro), or up to twice that amount in case of intentional infringement.

In addition, individuals may bring class action lawsuits based on privacy and data protection where the causes of action arise in the context of consumer or employment relations.

Fair processing information

Collection of personal data from a *data subject* must be accompanied by notice indicating: (i) whether delivery of the information by the *data subject* is voluntary or subject to a legal obligation; (ii) the purposes for which the information is collected; and (iii) any prospective transferees and the purposes of such transfer.

In addition, the *data subject's* consent must be "informed" and this has been interpreted by the courts to mean *data subjects* must have all relevant information concerning the processing of their data. Hence, while not expressly specified in the PPA, it is necessary to provide *data subjects* with a good understanding of which categories of personal data are being collected, used and transferred.

Rights to access information

Subject to certain limited exceptions, *data subjects* enjoy rights of access to their information.

Objection to direct marketing

Data subjects may object to (opt out of) direct marketing. They may also require that their personal data be deleted from a database used for direct marketing and not transferred from a database used for direct marketing services.

Other rights

Subject to certain limited exceptions, *data subjects* enjoy rights to rectify their information.

Security

Security requirements in order to protect personal data

The PPA makes database owners, possessors and managers all responsible for the information security of a database.

Information security requirements are further specified in the Security Regulations, which requires database managers to: (i) physically protect the automatic data processing system; (ii) establish procedures and rules for database management; (iii) control access permits for authorized personnel; (iv) require authorized personnel to execute a confidentiality agreement; (v) verify compliance with database operating procedures; (vi) implement security measures appropriate to the sensitivity of the data to prevent unauthorized disclosure or access thereto; and (vii) establish auditing procedures. Additional data security requirements apply to Limited Data.

ILITA has recently issued draft data security regulations which apply to both the public and private sectors, the draft Protection of Privacy Regulations (Information Security in Databases), 5770-2010 (the "**Draft Regulations**"). The Draft Regulations impose much stronger obligations including the appointment of an information security officer, conducting periodic risk assessments, documenting potential security breaches and imposing certain terms on outsourcing agreements. The Draft Regulations introduce not only detailed data security procedures but also wider privacy obligations, including limits on data retention and a requirement that data collected are relevant and not excessive. The regulations are modular, dividing databases into risk categories based on both data sensitivity and the number of *data subjects*, and applying different rules to "high", "medium" and "low" risk databases.

Specific rules governing processing by third party agents (processors)

The Security Regulations impose on the database manager an obligation to set forth data security procedures for *data processors*. Controllers typically satisfy this requirement by executing confidentiality agreements with service providers.

The Draft Regulations set forth specific provisions with respect to outsourcing and data processing by third parties. In addition, in June 2012, ILITA issued an instruction concerning data protection in the context of outsourcing.

Notice of breach laws

Breach notification obligations currently apply only in the financial sector under the Supervisor of Banks' Regulation No. 357 on Information Technology Management and equivalent instructions issued by the Commissioner of Capital Markets, Insurance and Savings.

The Schoffman Report called for the introduction into the PPA of wider breach notification obligations.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The PPA restricts data transfers to third parties, including corporate affiliates, within or outside of Israel. An additional layer of regulation applies to international data transfers under the Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel), 2001 (the "**Transfer Regulations**").

The Transfer Regulations apply to both inter- and intra-entity transfers of personal data outside of Israel. They permit transfers to: (i) EU Member States; (ii) other signatories of Council of Europe Convention 108; and (iii) a country "which receives data from Member States of the European Community, under the same terms of acceptance". This has been interpreted by the Database Registrar to apply to transfers to Safe harbor participant companies in the US.

Transfers to other countries are permitted: (i) subject to *data subject* consent; (ii) from an Israeli corporate parent to a foreign subsidiary; or (iii) provided the data importer "enters into a binding agreement with the data exporter to comply with Israeli legal standards concerning the storage and use of data".

Regardless of the basis for an international transfer, data exporters must also obtain the data importer's written undertaking that the data importer implements sufficient safeguards to protect individuals' privacy and promises to refrain from any onward transfer in its own country or any other country.

Notification and approval of national regulator (including notification of use of Model Contracts)

No notification of ILITA is required, other than as part of database registration.

Use of binding corporate rules

As specified above, the Transfer Regulations authorize transfers to a country "which receives data from Member States of the European Community, under the same terms of acceptance". This provision might be interpreted to authorize transfers to entities implementing EU-approved *binding corporate rules*.

Enforcement

Sanctions

A breach of data protection law (database registration; notification to *data subjects*) constitutes a strict liability criminal offense punishable by one year imprisonment and is also a civil tort.

ILITA is authorized to impose fines that accumulate daily up to approximately 70,000 USD (258,000 NIS). Under a November 2011 government sponsored legislative bill, ILITA would be authorized to impose civil penalties in an amount up to approximately 850,000 USD (3.2 million NIS).

Practice

ILITA has taken several enforcement actions in 2012, including for breach of purpose limitation; transparency; and direct marketing requirements. A list of enforcement actions is available on ILITA's website and a summary is contained in its annual report. ILITA's most important enforcement action over the past two years concerns a massive data breach involving the loss and eventual posting on the Internet of Israel's entire population registry consisting of more than 9 million records related to every Israeli citizen as well as those recently deceased. The investigation resulted in criminal indictments, which are currently pending in court, of government contractors as well as recipients of the data.

Fines have ranged up to several thousand NIS to 258,000 NIS (70,000 USD) in a case concerning illegal trading of personal data and 176,000 NIS (50,000 USD) in a case concerning illicit use of an illegal copy of the population register.

Individual lawsuits typically deal with privacy in the workplace, particularly monitoring of electronic communications, anti-spam legislation, data security breaches and privacy in the press. In an important decision from February 2011, the National Labour Court severely restricted employers' ability to monitor employee emails. The Court made strong statements concerning the suspect nature of employee consent and mandated the implementation of principles of legitimacy, transparency, proportionality, purpose limitation, access, accuracy, confidentiality and security. It stated that given the constitutional status of the right to privacy, exemptions to the PPA must be interpreted narrowly (Issakov v. Panaya).

Consumers have also brought several class action lawsuits, including against Apple for geolocation tracking mobile operator Pelephone for retention of SMS content and several Israeli companies for anti-spam violations.

In addition, contracts of adhesion (boilerplate) are subject to judicial scrutiny under the Standard Form Contract Act, 1982. In two recent cases, the Standard Contracts Tribunal invalidated clauses in standard form contracts purporting to secure customers' consent to the sharing of personal data among members of banking groups. It concluded that despite customer consent, data sharing practices were overly broad and therefore void.

In an August 2012 decision, the Tel Aviv District Court upheld the validity of an instruction issued by ILITA restricting financial institutions from using information about a third party's attachment of their client's account for the financial institution's own purposes. The court held that the regulator is authorized to issue market instructions interpreting the law. The decision is likely to have profound effects for the validity and weight given to this and other guidance documents and market instructions issued by ILITA. (Admin. App. 24867-02-11 IDI Insurance v. Database Registrar).

Enforcement authority

ILITA has authority for administrative enforcement actions. Criminal sanctions are only imposed by the courts.

Israel is a highly litigious society. Individual customer and employee lawsuits, including class action lawsuits, for privacy infringements are common.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The PPA and the Telecommunications Act (Telephone and Broadcast), 1982 ("**Telecom Act**").

Enacted in 2008, Section 30A of the Telecom Act is modelled after article 13 of the *Privacy and Electronic Communications Directive* and applies to businesses sending unsolicited commercial marketing messages by electronic means. It imposes strong civil and criminal penalties, including statutory damages, class actions, and directors' and officers' liability. It has also been pursued vigorously by individual plaintiffs.

Cookies

Conditions for use of cookies

No specific cookies legislation. If the cookie contains personal information it will be subject to the general provisions of the PPA.

Regulatory guidance on the use of cookies

None.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Section 30A of the Telecom Act prohibits the transmission of "advertising material" by electronic means without the recipient's prior explicit consent. That consent must be in writing.

Conditions for direct marketing by e-mail to corporate subscribers

Section 30A of the Telecom Act prohibits the transmission of "advertising material" by electronic means without the recipient's prior explicit consent. That consent must be in writing.

Exemptions and other issues

The Telecom Act provides two important exemptions. First, advertisers may contact a business (as opposed to an individual recipient) once to solicit consent for future communications.

Second, advertisers may transmit advertising material to an individual recipient if conditions very similar to the *similar products and services exemption* applies.

The Telecom Act regulates not only the means of transmission but also the content of advertising messages. Under the Telecom Act, an advertising message must be clearly labelled as such, using the word "advertisement" at the beginning of the message or, in case of an email message, the subject line. In addition, an advertising message must specify the name and contact details of the advertiser as well as the recipient's right to notify the advertiser at any time and by reasonable means of his or her refusal to receive additional messages. To avoid exceedingly long messages, the senders of SMS need only specify their name and contact details.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Under the PPA, individuals must be provided the opportunity to opt out of direct marketing, including having their personal data deleted from the database used to contact them.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The PPA applies only to individuals.

Exemptions and other issues

Transparency obligations under the PPA apply, as discussed above. In addition, the caller must disclose to the individual called the name and address of the controller of the database from which her contact details were drawn and the sources from which the controller of the database collected such information. In addition, databases should not be used for direct marketing services unless the person managing or possessing it has a record indicating the source from which the data was received, the date it was received, and to whom it was delivered.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The position is the same for marketing by e-mail. See above.

Conditions for direct marketing by fax to corporate subscribers

The position is the same for marketing by e-mail. See above.

Exemptions and other issues

The position is the same for marketing by e-mail. See above.

Italy.

Contributed by Gianni, Origoni, Grippo & Partners

General | Data Protection Laws

National Legislation

General data protection laws

The *Data Protection Directive* was originally implemented by the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data Act (No. 675 of 31 December 1996) ("**Law no. 675/96**"). However, Law no. 675/96 in 2004 has been replaced by the Consolidation Act regarding the Protection of Personal Data (Data Protection Code - Legislative Decree No. 196 of 30 June 2003) (the "**DPC**").

Entry into force

Law no. 675/96 came into force on 8 May 1997 and the DPC came into force on 1 January 2004.

National Regulatory Authority

Details of the competent national regulatory authority

Garante per la protezione dei dati personali (Italian Regulatory Authority) (the "**Garante**")
Piazza di Monte Citorio 121
00186 Roma
Italy

www.garanteprivacy.it

Notification or registration scheme and timing

The *data controller* has to submit a notification to the Garante before the commencement of certain kinds of personal data processing. No approval is required and notification is subject to a fee of EUR 150.

Exemptions

Notification is required only with regard to data processing which could jeopardise the rights and freedom of the *data subjects* because of the method of processing or the nature of the personal data it relates to. Accordingly, only *data controllers*: (i) in certain areas of activity such as health, direct marketing, credit referencing, telecommunications or user profiling; or (ii) carrying out certain kinds of processing expressly listed by the DPC, must notify their processing activities.

Appointment of a data protection officer

There is no current requirement under the DPC to appoint a data protection officer.

Personal Data

What is personal data?

The definition of personal data in the DPC is based on the *standard definition of personal data*.

The Garante has not adopted specific guidance but uses a broad approach to the definition of personal data in its decisions, in line with the *Opinion on Personal Data*.

Is information about legal entities personal data?

No. Under Law 214/2011 ("*Urgent measures for growth, equity and the consolidation of the public finances*"), data relating to legal entities, bodies or associations is excluded from the application of the DPC and information concerning such legal entities, bodies or associations does not fall within the *standard definition of personal data*. Therefore, legal entities, bodies and associations are no longer considered *data subjects*. However, there are specific rules applicable to legal entities, bodies and associations in relation to electronic marketing.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met or if certain other conditions are met, such as processing of data for economic activities in compliance with the legislation in force applying to business and industrial secrecy.

This condition relating to economic activities is frequently relied upon as grounds for processing non-sensitive personal data. In contrast, the legitimate interest condition is only used in situations expressly specified by the Garante (for example, in the case of video surveillance systems).

The DPC contains exemptions for certain types of processing. For example, processing carried out by natural persons for exclusively personal purposes is largely exempt from the provisions of the DPC.

Under the DPC, consent to processing is not required where processing: (i) is carried out to comply with an obligation set forth by law, regulation, EC provision or agreement; (ii) concerns data contained in public registers; (iii) is related to economic activities; or (iv) is aimed at the investigation of, claiming for or defence of a right in a legal action.

Recently (Law 106/2011), the Italian legislator has simplified the rules for data processing in relation to the communication of personal data carried out intra-group in cases where such communication is performed exclusively for financial-accounting purposes. Such intra-group communications are allowed without consent provided that the relevant *data subjects* have been informed by notice.

Are there any formalities to obtain consent to process personal data?

The DPC sets forth that consent: (i) must be free, specific and given for a clearly identified processing operation (which must be identified in an information notice to the *data subject*); and (ii) should be documented in writing for non-sensitive personal data but must be given in writing if the processing concerns sensitive personal data.

In accordance with the Guidelines issued by the Garante on 23 November 2006, the employees' consent is not necessary, under the legitimate interest exemption, provided the processing carried out by the employer is aimed at fulfilling the contractual employment relationship or complying with legal provisions, regulations or collective agreements.

Sensitive Personal Data

What is sensitive personal data?

Under the DPC, sensitive personal data means the *standard types of sensitive personal data*.

Are there additional rules for processing sensitive personal data?

Sensitive data may be processed only with both the *data subject's* written consent and the Garante's prior authorisation (though there are exceptions for religious bodies and trade unions). To this purpose, the Garante has issued several general authorisations for the processing of sensitive data.

Are there any formalities to obtain consent to process sensitive personal data?

Under the DPC, the consent of a *data subject* must be obtained in writing.

When processing sensitive personal data (including that of employees), the Garante Guidelines of 23 November 2006 concluded there was a legitimate interest in the processing of data concerning employees' health, and therefore this could be carried out without consent.

Scope of Application

What is the territorial scope of application?

The DPC applies the *standard territorial test*.

Who is subject to data protection legislation?

The DPC applies to anyone who processes personal data in Italy including *data controllers*, *data processors* and any person in charge of the processing.

Are both manual and electronic records subject to data protection legislation?

The DPC expressly provides that processing consists of any operation or set of operations regarding data, carried out with or without the help of electronic or automated means, whether or not the data are contained in a data bank. The information note provided to the *data subject* must indicate the mode of processing to be used.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation which includes pecuniary and non-pecuniary damage. A strict liability rule applies to this right to compensation.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects* and must also provide information about: (i) whether the supply of data is mandatory or voluntary; (ii) the possible consequences of refusal to consent to the data processing; (iii) the (categories of) entities to whom the data may be communicated or which may have access to the data as *data processors* or persons in charge of the processing; (iv) their rights as *data subjects*; and (v) the name and address of the *data controller* and the *data processor*. If several *data processors* have been designated, at least one among them shall be referred to and the mechanisms for accessing an updated list of *data processors* shall be specified.

The Garante may identify particular cases for simplified information arrangements (for example, for video surveillance activities, telephone services or collection of personal data by means of cookies).

The DPC does not provide any rules about the language of the information notices. However, considering its aims, they should be in a language spoken and understandable by the *data subject.*

Rights to access information

Data subjects may obtain their *subject access information* by making a request to the *data controller*, the *data processor* or the person in charge of the processing. This request is not subject to any formalities (i.e. it can be made by letter, facsimile or e-mail) and in some cases the request can be made verbally.

The *data subject* may be charged a fee if no personal data concerning the *data subject* is found. The fee shall not be in excess of the costs actually incurred for the inquiries made in the specific case and must be less than the limit specified by the Garante (see General Decision 23/12/04).

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing data for direct marketing purposes. The *data controller* must provide a response and cease processing data within 15 days, save that in some cases the request shall have to be complied with within 30 days.

Other rights

Data subjects may ask to have their personal data updated, amended or supplemented or have their personal data cancelled, transformed into anonymous data or blocked by the *data controller*. The Garante has specified that a *data subject* cannot ask for correction of data if the data are the result of an evaluation of the *data controller*.

Data subjects may object to the processing of their personal data on the basis of lawful reasons or even discretionally, in the case of commercial information, advertising material or market research.

Security

Security requirements in order to protect personal data

In addition to compliance with the *general data security obligations*, the DPC requires, under criminal sanction, the implementation of specific technical, logical and organisational minimum security measures set forth by a "Disciplinare Tecnico", contained in Annex B to the DPC.

Specific rules governing processing by third party agents (processors)

The processing of personal data by a *data processor* must be in accordance with a written appointment containing the *standard processor obligations*.

Notice of breach laws

The DPC does not contain any general obligation to inform the Garante or *data subjects* of a security breach.

However, the Garante set out specific provisions in relation to security breach notifications for the banking sector in its decision of 12 May 2011.

Furthermore, specific notice of breach laws apply to the electronic communications sector since the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive* have been implemented into national law by means of Legislative Decree Legislative Decree nr. 69 of May 28th 2012, imposing on electronic communication providers (such as ISP and telephone companies) certain obligations of data breach notification towards both the Garante and the *data subjects*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPC contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the *standard conditions for transborder dataflow*.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no obligation to notify the Garante or obtain his consent to use the *Model Contracts*. However, if the *data controller* uses an alternative set of contractual clauses, the Garante can determine adequate and specific protection for the *data subject's* rights under those alternative clauses.

Use of binding corporate rules

The DPC states that personal data can be transferred outside the EU with the authorisation of the Garante. Such authorisation will be granted if the Garante is satisfied there are safeguards for the rights of the *data subject* under the rules of conduct in place between group companies (*binding corporate rules*).

Enforcement

Sanctions

The Garante may impose administrative sanctions (fines) *inter alia* in cases of: (i) non-fulfilment of the obligation to provide the *data subject* with the Information Notice; or (ii) failure to notify or incomplete notification to the Garante.

The DPC provides for up to three years' imprisonment and publication of the judgment decision in the event of *inter alia*: (i) unlawful personal data processing, if damage occurs; (ii) false notification; or (iii) failure to adopt and implement the required security measures.

Practice

In 2011 the Garante decided 257 cases. These mainly related to the processing of personal data by social security institutions but also covered the telecommunications sector, public and private employers, scientific research and marketing activities.

In 2011, the Garante issued 358 orders and its activities mainly focused on: (i) the creation and commercialisation of databases for marketing purposes; (ii) unsolicited marketing calls, faxes and emails; (iii) customer care activities carried out by economic operators and call centers (including in relation to the transfer abroad of personal data); (iv) biometric and genetic data; (v) payments by means of credit card; (vi) journalism and online information; and (vii) data collection via websites e.g. forums dedicated to health).

Enforcement authority

With regard to any breach of the DPC provisions, the *data subject* may apply either to the Garante or ordinary Court. The Garante may order the data processing to be stopped or lay down conditions for the processing. Furthermore, the Garante may impose sanctions or administrative fines. In the event of crimes, the Garante has an obligation to inform the relevant criminal authorities.

Compensation for damages can be requested from the Civil Courts.

The Garante has powers of investigation and can also use the Financial Police ("**Guardia di Finanza**").

ePrivacy | Marketing and cookies

National Legislation

ePrivacy laws

The DPC implemented Article 13 of the *Privacy and Electronic Communications Directive*. The effective date was 1 January 2004.

Furthermore, with the approval of Legislative Decree nr. 69/2012, several provisions of the DPC have been amended to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Since the DPC has been amended to implement the *Citizens' Rights Directive*, it is necessary to inform users and to obtain their consent to the use of cookies, unless the cookie is strictly necessary for the provision of a service to that subscriber or user. To this extent, the user can be informed with simplified information, which will be determined by the Garante.

Regulatory guidance on the use of cookies

The Garante is in the process of providing regulatory guidance on the use of cookies. In November 2012 the Garante issued a public consultation addressed to institutions and operators in the telecommunication sector, aimed at finding the most suitable methods to provide users with a clear and simplified information notice on the collection and use of their personal data through cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Marketing or advertising communications by e-mail shall be permitted only with the consent of the recipient.

Conditions for direct marketing by e-mail to corporate subscribers

Marketing or advertising communications sent by e-mail shall be permitted only with the consent of the recipient, in its role as "user/contractor". Contrary to the meaning of *data subject*, the term "user/contractor" includes legal entities, bodies and associations and applies to all means of direct marketing.

Exemptions and other issues

The requirement for prior consent does not apply to e-mail marketing if the *similar products and services exemption* applies. For this exemption to apply then there must be a contractual relationship between the *data controller* and the *data subject* and the recipient's details must have been collected in connection with the negotiation for sale of products and services.

The DPC also prohibits direct marketing e-mails from being sent if the identity of the sender is disguised or concealed.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to individual subscribers who have not previously provided their consent to such kind of activities.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to corporate subscribers without their consent.

Exemptions and other issues

Consent is not necessary if one of the standard conditions for exemption from consent is met, including if the processing concerns data related to the economic activities of an addressee. In addition, the *data subject* can object to the processing for marketing purposes at any time.

It is worth noting that the Italian legislator has introduced a register for objections, the so-called "*Registro delle Opposizioni*", in which the "user/contractor", whose personal data are enrolled in the electronic or paper telephone directories, can register themselves in order to object to the processing of their personal data for marketing purposes (by telephone and by ordinary mail). *Data controllers* can, however, carry out marketing activities by telephone and by mail without "user/contractor" consent, provided that they subscribe to the register and match their lists of "user/contractor" with such register, to ensure they do not market to those "user/contractor" who have registered an objection.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send direct marketing faxes to individual subscribers without their consent.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send direct marketing faxes to corporate subscribers without their consent.

Exemptions and other issues

No exemptions apply.

Japan.

General I Data Protection Laws

National Legislation

General data protection laws

Japan is not an EU Member State and therefore has not implemented the *Data Protection Directive*. However, the Act on the Protection of Personal Information (Act No. 57 of 30 May 2003) (the "**APPI**") contains similar provisions to those in the *Data Protection Directive*.

Entry into force

The majority of the provisions of the APPI came into force on 1 April 2005.

National Regulatory Authority

Details of the competent national regulatory authority

The Consumer Affairs Agency has overall responsibility for the legal framework of the APPI.

Consumer Affairs Agency
Sanno Park Tower
11-1, Nagatacho 2-chome
Chiyoda-ku
Tokyo 100-6178

www.caa.go.jp

In addition, each regulatory authority, such as the Financial Services Agency and Ministry of Economy, Trade and Industry, has authority to advise, recommend or order the businesses it supervises to comply with the APPI.

Notification or registration scheme and timing

There is no requirement to make any notifications to the regulatory authority. However, the relevant authority can order an information handler to submit a report to the authority on the treatment of personal information.

Exemptions

Not applicable.

Appointment of a data protection officer

The APPI does not specifically require the appointment of data protection officers. However, the Financial Services Agency of Japan's guidelines (the "**FSA Guidelines**") require financial institutions to appoint data protection officers. The Ministry of Economy, Trade and Industry of Japan's guidelines (the "**METI Guidelines**") recommend that a company appoint a chief privacy officer.

Personal Data

What is personal data?

The APPI defines personal information as information about a living person that would allow identification of the person as an individual. This includes such information as will allow easy reference to other information and will thereby enable the identification of the specific individual.

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

As a general rule, information handlers must: (i) specify so far as possible the purpose for which personal information will be processed ("**purpose of use**"); (ii) not change the purpose of use such that it no longer has a reasonable relationship to the original purpose of use; (iii) not process personal information except to the extent required to achieve the purpose of use without the prior consent of the *data subject*; and (iv) when they obtain personal information as a result of succession to the business of another information handler, not process personal information without the prior consent of the *data subject*, except to the extent required to achieve the purpose of use prior to the succession.

An information handler may not transfer personal information to a third party without prior consent of a *data subject*.

Are there any formalities to obtain consent to process personal data?

Consent is not generally required to process personal information. However, prior consent (oral or written) is needed for processing outside the scope of the original purpose of use.

Financial institutions handling personal information are required by the FSA Guidelines to obtain consent to a change of purpose of use in writing.

Sensitive Personal Data

What is sensitive personal data?

The APPI does not distinguish between different types of personal information based on the sensitive nature of such data. However, certain guidelines (including the FSA Guidelines) stipulate additional rules for processing sensitive personal information such as information relating to an individual's political views, faith, labour union membership, race, ethnic group, family status, physical/mental handicap, sex life, criminal records and medical records.

Are there additional rules for processing sensitive personal data?

Certain guidelines (including the FSA Guidelines) provide that the relevant information handlers may not acquire, hold, use or transfer sensitive personal information except where strictly necessary. The rules vary slightly in each guideline.

Are there any formalities to obtain consent to process sensitive personal data?

Not applicable.

Scope of Application

What is the territorial scope of application?

The APPI applies to information handlers: (i) which have their residences or offices (for example, headquarters or a branch) in Japan; or (ii) which are non-Japanese companies and carry on business in Japan.

Who is subject to data protection legislation?

Japanese law does not contain the concepts *data controller* and *data processor*. The APPI instead uses the concept of an "information handler". This is any person or entity that possesses and uses for its business in Japan a database which contains personal information on more than 5,000 individuals on any day in the most recent six month period.

The FSA Guidelines require financial institutions to make every effort to comply with the FSA Guidelines even if an entity possesses personal information on 5,000 or fewer individuals.

Are both manual and electronic records subject to data protection legislation?

The APPI applies to both manual and electronic records.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation for damages, including mental distress.

Fair processing information

Information handlers are required to make available to *data subjects* the following information (and must reply to a *data subject's* request for such information without delay): (i) the information handler's name; (ii) purpose of use of the *data subject's* personal information; (iii) procedures for requesting access to personal information held by the information handler (including the amount of any fees payable); and (iv) details of whom to contact in order to lodge complaints concerning the handling of their personal information.

An information handler who has acquired personal information is required to promptly notify *data subjects* of the purpose of use of their personal information, except in cases where the purpose of use has already been publicly disclosed. When an information handler has changed the purpose of use, it must notify the *data subject* of the changed purpose of use or publicly announce such changed purpose of use.

An information handler is required to publish the privacy policy on its website or post or display copies of the privacy policy in its reception or other prominent position at its offices.

Rights to access information

An information handler is required to notify *data subjects* of the purpose of use of their personal information upon their request.

An information handler is required, upon a *data subject's* request, to disclose such retained personal information as may lead to the identification of the *data subject* without delay.

An information handler may collect reasonable charges for the notification or disclosure mentioned above.

Objection to direct marketing

The APPI does not provide any specific rights to reject direct marketing. However, information handlers must not process personal information except to the extent required to achieve the purpose of use, without the prior consent of the *data subject*.

Other rights

Data subjects may require an information handler to correct, add to or delete their personal information if such information is not factually correct.

Data subjects may require an information handler to cease using or erase their personal information if such personal information is being used beyond the purpose of use without their consent, or was obtained by unfair means. The information handler may refuse such request if compliance with such request would cause the information handler to incur excessive costs, or where it would otherwise be difficult for the information handler to discontinue using or to erase the personal information, provided that the information handler takes necessary alternative measures to protect the rights and interests of the *data subject*.

Security

Security requirements in order to protect personal data

Information handlers are required to implement appropriate control measures in respect of the personal information in their possession to prevent unauthorised disclosure, loss or damage of such personal information.

Specific requirements for appropriate control measures are provided in the guidelines issued by the regulatory authorities.

Specific rules governing processing by third party agents (processors)

When an information handler entrusts a third party with the handling of personal information in whole or in part, the information handler must exercise necessary and appropriate supervision over the third party to ensure the security of the entrusted personal information.

Notice of breach laws

In general, there is no notice of breach obligation under the APPI. However, the FSA Guidelines require financial institutions handling personal information to: (i) report any incident including information leakage to the Financial Services Agency immediately; (ii) publish the factual details of the incident and measures to be taken to prevent a recurrence; and (iii) notify the facts of the incident to the relevant *data subject*. The METI Guidelines also recommend establishing a reporting system whereby any incident such as information leakage is notified to the relevant authority.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The APPI does not distinguish between third parties in Japan and overseas, and there are no specific provisions dealing with *transborder dataflows*.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no requirement to make any notifications to or obtain any approvals of the regulatory authority.

Use of binding corporate rules

No concept of *binding corporate rules* is used in the APPI.

Enforcement

Sanctions

Breaches of the APPI and/or related regulatory guidelines may result in civil liability or criminal sanctions, which include up to six months' imprisonment or a fine of up to 300,000 Japanese yen.

A breach of the APPI and/or related regulatory guidelines would not, of itself, be a criminal offence. However, a breach of the APPI and/or related regulatory guidelines may result in the relevant regulatory authority issuing an enforcement notice ordering the information handler to cease or improve data handling. A failure by the information handler to comply with such enforcement notice would be a criminal offence.

Practice

The relevant regulatory authority normally first recommends that an information handler cease the violation and take other necessary measures to correct the violation. If the information handler does not take the recommended measures without good reason, the relevant regulatory authority may then order the information handler to take the recommended measures.

The number of enforcement actions taken in the past is not clear. However, according to the Financial Services Agency's publication, it issued four recommendation orders during the period since the APPI came into force until the end of June 2011. The webpage of the Ministry of Economy, Trade and Industry indicates three entities were ordered to report the factual background of information leakage in the twelve month period to September 2011.

Enforcement authority

The relevant regulatory authority in respect of an information handler is the government ministry with jurisdiction over the business of the information handler. That regulatory authority has no power to take direct enforcement action other than by issuing enforcement notices. Importantly, the regulatory authority itself has no ability to impose criminal penalties on information handlers.

A criminal prosecution against a person who fails to comply with an enforcement notice needs to be brought before a Japanese court.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Japan is not an EU Member State and, therefore, has not implemented the *Privacy and Electronic Communications Directive*. However, the Act on Specified Commercial Transactions (Act No. 57 of 4 June 1976) (the "**ASCT**") and the Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 17 April 2002) (the "**ARTSEM**") provide restrictions on direct marketing.

Cookies

Conditions for use of cookies

There are no special rules for cookies. If information collected by using cookies allows identification of an individual by reference to other information already available to a website owner, the owner is required by the APPI to notify the individual directly or publish the purpose of use of the personal information.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

It is only possible to send direct marketing e-mails to individual subscribers if they consent.

Conditions for direct marketing by e-mail to corporate subscribers

It is only possible to send direct marketing e-mails to corporate subscribers if they consent.

Exemptions and other issues

Under the ARTSEM, it is permitted to send e-mails for the purpose of direct marketing without consent if: (i) the recipient notifies the sender of its e-mail address in writing; (ii) the recipient has a business relationship with a person engaged in sales activities relating to the marketing; or (iii) the recipient is an organisation or an individual engaged in business who discloses its e-mail address on the Internet.

Under the ASCT, it is permitted to send e-mails for the purpose of direct marketing without consent in connection with certain types of sales transactions if: (i) such e-mail for direct marketing is sent in association with notifications of important matters relating to contracts; or (ii) such e-mail for direct marketing is sent together with emails from free email providers, such as Yahoo! or Google.

The sender of the e-mail must be identified by providing its name and address. The sender also needs to provide the receiver's right to opt out of further marketing emails and provide email address or URL in order to opt out.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to solicit a sales contract or a service contract from an individual subscriber who has expressed his/her intention not to enter into a sales contract or a service contract.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to solicit a sales contract or a service contract from a corporate subscriber which has expressed its intention not to enter into the sales contract or a service contract.

Exemptions and other issues

When a product seller or a service provider solicits customers for their products or services by means of telephone communication, it is required to inform the recipient of the following information prior to the solicitation: (i) its name and address; (ii) the name of the person in charge of the solicitation; (iii) the type of product or service being offered; and (iv) the purpose of the telephone call (i.e., to solicit the custom of the recipient).

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

There are no specific rules relating to unsolicited direct marketing by facsimile.

Conditions for direct marketing by fax to corporate subscribers

There are no specific rules relating to unsolicited direct marketing by facsimile.

Exemptions and other issues

Not applicable.

Latvia.

Contributed by LAWIN

General I Data Protection Laws

National Legislation

General data protection laws

The Law on Protection of Personal Data of Natural Persons (the "**DPA**") was adopted on 23 March 2000. The DPA incorporates the principles and provisions of the *Data Protection Directive*.

Entry into force

The DPA came into force on 20 April 2000.

National Regulatory Authority

Details of the competent national regulatory authority

State Data Inspection (the "**SDI**")
Blaumana 11/13 – 15,
Riga, LV-1011,
Latvia

www.dvi.gov.lv

Notification or registration scheme and timing

Under the DPA, and unless the processing is exempt, all state and municipal authorities and other natural and legal persons who perform or wish to commence personal data processing must register such processing with the SDI. The SDI reviews the information submitted and, if necessary, performs a pre-registration examination. Registration is subject to payment of state fee of LVL 20 for natural persons and LVL 40 for legal persons.

Exemptions

Exemptions from registration of processing apply in respect of: (i) processing for accounting and personnel registration needs; (ii) processing done by religious organisations; (iii) processing for journalistic purposes; (iv) processing for archival purposes; (v) processing within state or municipal information systems, the data of which are publicly available; (vi) processing where the *data controller* has a registered data protection officer; (vii) processing for scientific, genealogic or statistical research purposes; and (viii) where processing is based on the consent of the *data subject* or it arises out of contractual relations.

However, the exemptions do not apply if processing: (i) involves the transfer of personal data outside of EU or EEA states; (ii) is related to the rendering of financial services, market or public opinion polls, recruitment or assessment of personnel services as a business activity, lotteries or draws; (iii) involves information on persons' health; and (iv) involves information relating to unlawful activities, or criminal or administrative violation records.

Appointment of a data protection officer

There is no obligation to register personal data processing if the *data controller* has registered a data protection officer with the SDI.

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. In February 2009, the SDI published "Personal Data Definition" guidelines which, according to its foreword, are based on the *Opinion on Personal Data* and the experience of the SDI and authorities of other EU member states.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met.

The DPA contains exemptions for certain types of processing. For example, the DPA does not apply at all if processing is done by natural persons for personal, family or household purposes and the data are not exposed to third parties. Certain provisions of the DPA are not applicable if processing is for journalistic purposes.

Are there any formalities to obtain consent to process personal data?

The DPA does not specify any formal requirements for consent, except that consent has to be in writing if the *data controller* is processing sensitive personal data. However, it is advisable to obtain consent in a recordable form for evidential purposes irrespective of the type of personal data.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data means the *standard types of sensitive personal data*.

Criminal records and personal identification codes are regarded as a specific type of personal data which require satisfaction of additional conditions for their processing but are not regarded as sensitive personal data. Biometric data are recognised as personal data, but not as sensitive personal data, therefore no additional requirements for their processing apply.

Are there additional rules for processing sensitive personal data?

There is a general ban for the processing of sensitive personal data. As an exception, sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met or one of the alternative grounds set out in Latvian law is satisfied.

The alternative grounds are that processing is necessary for: (i) rendering social aid; (ii) developing the Latvian national archives; (iii) statistical surveys performed by the Central Statistical Bureau; (iv) performance of administrative functions or developing the state information systems; or (v) an insurance contract.

Are there any formalities to obtain consent to process sensitive personal data?

Consent for the processing of sensitive personal data must be in writing. There is no concept of implied consent when it comes to sensitive personal data.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The DPA applies to any person that can be regarded as the *data controller*. The *data controller* is responsible for compliance with the DPA.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to any processing of personal data, irrespective of the form. It can be either a manual filing or electronic system and at the same time it need not be a system at all.

Rights of Data Subjects

Compensation

If a *data subject* has suffered any loss or damage as a result of a violation of the DPA, he/she has the right to receive a reimbursement for that loss or damage from the *data controller*.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. This includes an obligation to provide details of any *data processors*. Upon request of the *data subject*, the *data controller* has an obligation to provide information about prospective recipients of the personal data. Pursuant to State Language Law, any information that must be provided by law has to be provided in the Latvian language.

Rights to access information

Data subjects may obtain their *subject access information* by request to *data controllers*. The law stipulates that twice a year such information shall be provided free of charge, and the response of a *data controller* must be in writing. This right is subject to a range of statutory exceptions.

Objection to direct marketing

Unless the law states otherwise, a *data subject* may request that a *data controller* stops processing its data for commercial purposes, including processing for marketing purposes.

Other rights

A *data subject* has the right to request that his personal data are updated or adjusted, as well as their processing is ceased or the data are destroyed, if the personal data are incomplete, outdated, false, illegally obtained, or they are not necessary for collection purposes any more. If the *data subject* can verify such conditions, the obligation of the *data controller* is to promptly remedy such deficiency or violation and notify thereon any third parties who have received the processed data previously.

Security

Security requirements in order to protect personal data

The *data controller* and the *data processor* must comply with the *general data security obligations*. The mandatory technical and organisational requirements for protection of personal data in the course of processing are established by the Cabinet of Ministers of the Republic of Latvia in the form of specific regulations.

Specific rules governing processing by third party agents (processors)

Data controllers may entrust processing of personal data to *data processors* under a written agreement. *Data processors* may only process data as provided in the agreement and *data controllers* shall ensure that *data processors* obey the DPA, including the *general data security obligations*. The *data controller* has to identify its *data processors* in the application for registration of data processing to the SDI.

Notice of breach laws

The DPA does not oblige the *data controller* to notify the *data subject* or the SDI about a security breach. However, *data controllers* in specific sectors may be required to file notifications with other regulators relating to personal data breaches, adverse events and important developments or similar (for example, banks shall notify the Finance and Capital Market Commission).

Specific notice of breach laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. This has been implemented in Latvia through the Electronic Communications law ("**ECL**"). The ECL requires electronic communications providers ("**ECP**") to notify SDI of personal data breaches which occur on their electronic communications networks. ECP's must also notify the *data subjects*, if they may be negatively affected by such a breach. Notification of the *data subjects* is not necessary if the ECP can prove to SDI that the data concerned was encrypted and cannot be accessed by the third party who has obtained that data. The ECP must keep information about any security breaches for 18 months from their occurrence.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains restrictions on *transborder dataflows*. Personal data can be transferred to another country only if that country ensures the level of data protection which corresponds to the level of data protection effective in Latvia. In general, only EEA countries are regarded as having an adequate level of protection. However, personal data may also be transferred to a country that does not ensure the same level of protection if the *data controller* undertakes to supervise fulfilment of the relevant protection measures and at least one of the following preconditions is complied with: (i) consent of the *data subject* is obtained; or (ii) transfer of data is necessary in order to fulfil an agreement between the *data subject* and the *data controller*, whereupon the personal data shall be transferred in accordance with the contractual liabilities of the *data subject*; or (iii) transfer of data is necessary and requested under the set procedure in accordance with significant national and public interests, or is necessary for litigation; or (iv) transfer of data is necessary in order to protect the life and health of the *data subject*; or (v) transfer of data applies to public data or data collected in a publicly available registry.

For the *data controller* to be able to supervise fulfilment of the respective protection measures, the *data controller* and the recipient of the personal data shall enter into a contract on transfer of personal data. Provisions to be included in the contract for the transfer of personal are established by the Cabinet of Ministers.

Notification and approval of national regulator (including notification of use of Model Contracts)

In case of data transfers outside the EU/EEA, to a country that has not already been recognised as ensuring adequate level of protection, the assessment of the protection level in the receiving country is made by the SDI, which issues a written consent to the transfer of personal data. If an adequate level of protection is not established, data transfers to such a country can occur only via Model Contract, *binding corporate rules* or if the recipient is Safe Harbor certified. In all cases where data are to be transferred to a country without adequate level of protection, transfers cannot commence before data processing registration with the SDI.

Use of binding corporate rules

Although the DPA does not mention the use of *binding corporate rules* for *transborder dataflows*, the SDI is a member of the mutual recognition club for *binding corporate rules* and has published a recommendation allowing multinational

companies to adopt *binding corporate rules* as a means of ensuring adequate levels of data protection. However: (i) the *binding corporate rules* must be approved by the SDI or by the respective regulator in another EU Member State; and (ii) the local *data controller* must be registered with the SDI.

Enforcement

Sanctions

The SDI has the right to impose administrative fines or issue warnings for violations of the DPA. These fines range from LVL 50 to LVL 500 for individuals and from LVL 1,000 to LVL 10,000 for legal entities.

Recently, criminal liability has been introduced for the unlawful processing of personal data. The criminal law imposes sanctions of: (i) up to two years' imprisonment or forced labour, or a fine of up to 100 minimum monthly salaries (currently, the minimum salary in Latvia is LVL 180 or roughly EUR 250), for illegal use of personal data if material damage has been done; (ii) up to four years' imprisonment or forced labour, or a fine of up to 120 minimum monthly salaries, for illegal use of personal data by a *data controller* or *data processor*, if committed for the purposes of revenge, greed or blackmail; and (iii) up to five years' imprisonment or forced labour, or a fine of up to 200 minimum monthly salaries, for using violence, threats or deception against a person with intent to carry out any unlawful use of personal data.

Practice

According to the latest public report of 2011, the SDI received 257 complaints and performed 290 reviews regarding possible violations of the DPA. The number of cases has steadily increased year on year. In 2011 violations were established and administrative penalties, including both fines and warnings, were applied in 47 cases (23 monetary penalties and 24 warnings). These cases mostly concerned publication of data on the internet, provision of personal data of another person instead of own data and improper video surveillance. The public report of 2012 is not yet available.

Enforcement authority

As of 1 July 2009 the *data subject* must first contact *data controller* with its complaint on data processing. Only if the *data subject* and the *data controller* cannot resolve the issue themselves, the *data subject* may file a complaint with SDI.

Complaints concerning violations in the field of personal data protection are reviewed by the SDI, which is also authorised to impose penalties. A report on the alleged violation of personal data protection is prepared by the inspector of the SDI or other SDI employee who initiates examination of the case. Following completion of the examination of the case, the director of the SDI or the administrative punitive commission of the SDI makes a decision, imposing either a penalty or issuing a warning. The type of sanction depends on the severity of the violation and can either be a warning, fine or prohibition on data processing. Currently, violations of the DPA result in administrative liability in accordance with the Code of Administrative Offences of Latvia.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Latvian ePrivacy laws are contained in the Electronic Communications Law (the "**ECL**") and the Law on Information Society Services (the "LISS"), both of which implemented Article 13 of the *Privacy and Electronic Communications Directive*. The ECL stipulates the allocation of supervisory functions for the electronic communications market. The ECL provides for the protection of user data, including the protection of personal data in the field of electronic communications services. The LISS ensures free movement of information services in the EEA countries, specifies the cases in which the service supplier may offer information society services, lists the scope of information to be provided to the recipient of a service, as well as determines the liability and obligations of suppliers of agency services. Compliance with the law is supervised by the Consumer Rights Protection Centre (the "**CRPC**") and the SDI.

The ECL and LISS were amended on 19 May 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

The LISS requires that a cookie can only be placed on the end-user's device after the user has been provided with clear and comprehensive information, in accordance with DPA, about the purposes of the processing, and has consented to that use. Consent is needed for the use of cookies, unless the cookie is strictly necessary for the provision of a service requested by that subscriber or user or for transfer of information within an electronic communications network. The LISS does not expressly refer to the use of browser settings as a means of obtaining consent. There is an express requirement for consent to be "prior" to the use of a cookie.

Regulatory guidance on the use of cookies

Currently, there is no official regulatory guidance from SDI about the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Sending commercial notices to an individual contact by e-mail is prohibited under Latvian law if the recipient of a service has not given a prior, free and clear consent to the receipt thereof. In accordance with the LISS, a commercial notice means any notice in electronic form that is intended for direct or indirect advertising of goods and services. However, a notice providing direct access to the general information on a service supplier and its activities, for example, a domain name or e-mail address, is not deemed to be a commercial notice.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing by e-mail to corporate subscribers (legal entities) is permitted as long as an option to unsubscribe is provided in each e-mail. There is no need for prior approval.

Exemptions and other issues

The *similar products and services exemption* applies. The LISS also prohibits the use of e-mail to send commercial notices if the identity of the sender is hidden or concealed or an invalid e-mail address is used.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Giving commercial notices to individual subscribers by telephone is prohibited under Latvian law if the recipient of a service has not given a prior, free and clear consent to the receipt thereof.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The law does not require obtaining prior approval from legal entities to use marketing by telephone. However, requests to discontinue such calls in future still have to be respected.

Exemptions and other issues

Invalid or concealed phone numbers cannot be used when marketing by telephone.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Giving commercial notices to individual subscribers by fax is prohibited under Latvian law if the recipient of a service has not given a prior, free and clear consent to the receipt thereof.

Conditions for direct marketing by fax to corporate subscribers

The position is the same as for marketing by telephone.

Exemptions and other issues

Invalid or concealed fax numbers cannot be used when marketing by fax.

Liechtenstein.

Contributed by Wanger Advokaturbüro

General | Data Protection Laws

National Legislation

General data protection laws

The Data Protection Act (the "**DPA**") dated 14 March 2002 and the relevant Ordinance on the Data Protection Act (Data Protection Ordinance, "**DPO**") dated 9 July 2002, implemented the *Data Protection Directive*.

Entry into force

The DPA came into force on 1 August 2002.

National Regulatory Authority

Details of the competent national regulatory authority

Datenschutzbeauftragter ("**The Data Protection Commissioner**")
Dr. Philipp Mittelberger
Data Protection Unit (*Stabsstelle für Datenschutz*)
Kirchstrasse 8
Post box 684
FL-9490 Vaduz
Liechtenstein

http://www.dss.llv.li

Notification or registration scheme and timing

Under the DPA, *data controllers* in the private sector who regularly: (i) process sensitive data; (ii) process personal profiles; or (iii) communicate personal data to a third party must notify the Data Protection Commissioner prior to processing if this operation is not subject to a legal requirement or the persons affected are unaware that such data are being processed. The Data Protection Commissioner is in charge of the register of data collections.

Data controllers in the public sector must notify the Data Protection Commissioner in all cases.

Exemptions

The Government may make exceptions to the notification obligation.

Appointment of a data protection officer

According to the DPA it is optional to appoint a data protection officer. This officer will be registered at the data protection unit and some duties are then delegated to him, such as keeping a list of the collected data.

Personal Data

What is personal data?

The definition of personal data in the DPA is based on the *standard definition of personal data*.

Is information about legal entities personal data?

Yes. The DPA applies to both individuals and legal entities.

What are the rules for processing personal data?

The processing conditions in the DPA distinguish between *data controllers* in the private and public sector. *Data controllers* in the private sector must satisfy processing conditions that are broadly similar to the *standard conditions for processing personal data*. For example, instead of a legitimate interest condition, there is a right to process data if there is an overriding public or private interest.

The processing conditions for *data controllers* in the public sector are far more restrictive and they may only process data if there is a legal basis to do so.

Are there any formalities to obtain consent to process personal data?

If required, consent is only valid if the *data subject* is given full information about the circumstances of the processing and such consent only extends to those circumstances.

Sensitive Personal Data

What is sensitive personal data?

Sensitive personal data include: (i) the *standard types of sensitive personal data* (though these do not include trade union information); (ii) social security files; and (iii) criminal or administrative proceedings and penalties.

The processing for "personality profiles", which are a collection of data that allow the appraisal of fundamental characteristics of the personality of a natural person, is also subject to additional controls.

Are there additional rules for processing sensitive personal data?

Both sensitive personal data and data constituting a personality profile are subject to specific rules. A private sector entity may only process sensitive data if the *standard conditions for processing sensitive personal data* are satisfied.

A public sector entity may only process sensitive personal data if: (i) it is indispensible in order to fulfil a specific legal obligation; (ii) the Government has authorised the processing; or (iii) the *data subject* has granted express consent or made the information public.

Are there any formalities to obtain consent to process sensitive personal data?

The consent of the *data subject* must be explicit.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The *data controller* is primarily responsible for compliance with the DPA. However, *data processors* also have an obligation to comply with the DPA and must respect the privacy of persons affected.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to both manual and electronic records, as it does not differentiate between the two.

Rights of Data Subjects

Compensation

Data subjects may be entitled to compensation if they suffer damage as a result of a breach of the DPA. This is especially the case if the person in breach of the DPA is a private sector entity.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects,* which must include information about: (i) the categories of data processed; (ii) the recipients of the data; or (iii) the *data subject's* rights to information and correction.

If the personal data have been obtained from a third party rather than the *data subject*, then the *fair processing information* need not be provided if: (i) it would involve unreasonable expense; or (ii) the processing is necessary for compliance with a legal obligation or research.

Rights to access information

Data subjects should, as a general rule, obtain their *subject access information* by written request to *data controllers*. The requested information will be basically provided free of charge. The information should, as a general rule, be submitted within 30 days in writing in printed form or as a photocopy. The right of access to personal data may be pursued under a special non-contentious civil proceeding (*AusserstreitverfahrenG*).

Objection to direct marketing

A *data subject* may require that a *data controller* stop processing data for direct marketing purposes. *Data subjects* also have to be notified in the event data are processed for the purpose of direct marketing.

Other rights

Data subjects have the right to require the rectification, erasure or blocking of personal data if the data are incomplete or inaccurate.

Unless the processing is authorised by law, *data subjects* have the right to object to the processing by the *data controller* of personal data on the grounds of predominant interests which are worthy of protection and which relate to the *data subject's* particular situation. Where there is a justified objection, the processing undertaken by the *data controller* may no longer involve the personal data in regard to which the objection was made.

Security

Security requirements in order to protect personal data

Data controllers must comply with the *general data security obligations*.

Specific rules governing processing by third party agents (processors)

The processing of personal data may be entrusted to a *data processor* provided: (i) the *data controller* ensures that no processing occurs that it would not be permitted to carry out itself; and (ii) the processing is not prohibited by a legal or contractual duty of confidentiality. Some parts of the contract between the *data processor* and the *data controller* must be documented in written or another permanent form.

The *data processor* will be subject to the same duties and may assert the same grounds of lawful justification as the *data controller*.

If personal data are to be shared with other *data processors* abroad, written contracts are necessary to limit the disclosure, processing and sharing to between other companies who support the service of the *data controller* or owner of the data.

Notice of breach laws

The DPA does not contain any obligation to inform the Data Protection Commissioner or *data subjects* of a security breach. However, *data controllers* in certain sectors may be required to inform competent regulators of any breach.

Specific notice of breach laws will apply to the electronic communications sector once the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive* have been implemented into national law.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Save for transfers to whitelisted countries, personal data may not be transferred outside of the EEA if the privacy of the persons affected could be seriously endangered. This applies especially if these countries do not have data protection laws granting a similar level of protection to those in Liechtenstein.

Notification and approval of national regulator (including notification of use of Model Contracts)

The Data Protection Commissioner must be notified of any *transborder dataflow* unless: (i) there is a legal obligation to disclose the data and the persons affected have knowledge of the transmissionor; or (ii) the transmission of files is to a state with equivalent data protection legislation (see Annex 2 to the DPO) and the files do not contain sensitive data or personal profiles.

In particular, the Data Protection Commissioner has to be notified if *Model Contracts* are being used.

Use of binding corporate rules

Although the Data Protection Commissioner supports the use of *binding corporate rules* there is no formal recognition of them currently as a means to justify *transborder dataflows*.

Enforcement

Sanctions

Private individuals who wilfully breach the DPA can receive a fine of up to CHF 20,000 and be imprisoned for up to three months in the event the fine is not paid.

A person who wilfully breaches the DPA in the context of his professional activities can be imprisoned for up to one year or fined up to 360 daily rates (which is a figure calculated by reference to the income of the offender).

Practice

In the year 2011, the Data Protection Commissioner dealt with 559 inquiries in total. This is an increase of 36 on the 523 inquiries received in 2010. Information about the numbers of investigations and penalties imposed is not published.

Enforcement authority

The Data Protection Commissioner can investigate cases on his own initiative or at the request of third parties. For this purpose he may request the production of documents, obtain information and have data processing activities explained to him. On that basis the Data Protection Commissioner may recommend improvements and in some cases he also may inform the government about such recommendations.

However, civil procedures and prosecutions for criminal offence can only be carried out by the Princely Court.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Communication Act dated 17 March 2006, which came into force on 6 June 2006 (the "**CA**"), implemented Article 13 of the *Privacy and Electronic Communications Directive*.

The CA has not been amended yet to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. The implementation will be arranged by the Office for Communication as the regulatory, supervisory administrative authority for telecommunications in Liechtenstein in the fields of telecommunication, radio, television, cable television and Internet.

Cookies

Conditions for use of cookies

Currently, it is only necessary to inform users of the use of cookies and offer them the right to refuse their use. However, when the CA is amended to implement the *Citizens' Rights Directive* it will be necessary to obtain consent to the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user.

Regulatory guidance on the use of cookies

None.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under the CA it is not permitted to transmit messages for the purpose of direct marketing by e-mail unless the recipient has previously consented explicitly to the transmission. In addition, an organisation can send one single e-mail to customers asking them if they consent to further direct marketing.

Conditions for direct marketing by e-mail to corporate subscribers

The same conditions apply as for direct marketing by e-mail to individual subscribers.

Exemptions and other issues

Under the CA it is permitted to transmit messages if the *similar products and services exemption* applies. Notwithstanding this exemption or the receipt of consent from the recipient, the transmission of messages is not permitted if: (i) the recipient's contact details have been obtained by chance; (ii) the sender is informed or should be informed about the recipient's subsequent refusal of consent; or (iii) the transmission violates any other provision of Liechtenstein law.

Finally, the CA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Under the Distance Selling Act it is only permitted to make direct marketing calls to customers if they would not obviously object to that call. This provision is only applicable to telecommunications between an individual subscriber and a seller of goods or services where such telecommunication is used for the initiating and signing of a contract relating to such goods and services.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

There are no relevant provisions.

Exemptions and other issues

There are exemptions for agreements relating to: (i) the partial utilisation of a residential building; (ii) the supply of financial services according to the Distance Financial Services Act; (iii) the building and selling of real estate or other rights of real estate not including letting; (iv) the delivery of groceries, beverages and other household articles of daily use, which are delivered by the seller to the customer's domicile, whereabouts or place of employment in the framework of frequent and recurring delivery drives; and (v) the supply of services in the range of accommodation, carriage, delivery

of meals and drinks as well as recreational activities, if the seller engages at the time of contracting to render service at a certain time or within a certain time limit.

According to the Distance Selling Act a caller should identify themselves to the recipient.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Under the CA it is not permitted to transmit messages for the purpose of direct marketing by fax unless the recipient has previously consented explicitly to the transmission.

Conditions for direct marketing by fax to corporate subscribers

The same conditions apply as for direct marketing by fax to individual subscribers.

Exemptions and other issues

Under the CA it is permitted to transmit messages for the purpose of direct marketing by fax where the recipient (as the sender's customer) has provided to the sender his contact details in accordance with the *similar products and services exemption* and has not objected to their use for direct marketing. In order to obtain consent the sender shall transmit a relevant request by fax. In this request, the sender must include in clear, explicit and noticeable form information that the recipient is entitled to refuse each further fax.

Notwithstanding this exemption or the receipt of consent from the recipient, the transmission of messages is not permitted if: (i) the recipient's contact details have been obtained by chance; (ii) the sender is informed or should be informed about the recipient's subsequent refusal of consent; or (iii) the transmission violates any other provision of Liechtenstein law.

Lithuania.

Contributed by LAWIN

General | Data Protection Laws

National Legislation

General data protection laws

The Law on Legal Protection of Personal Data dated 11 June 1996 (as modified on 17 July 2000, 22 January 2002, 21 January 2003 and overhauled as of 1 January 2009 with subsequent amendments on 1 September 2011) (the "**DPA**") implemented the *Data Protection Directive*.

Entry into force

The latest modifications to the DPA came into force on 1 September 2011. They include amendments and new regulations on public polls, credit referencing agencies and specifics of the regulator's status.

National Regulatory Authority

Details of the competent national regulatory authority

The State Data Protection Inspectorate (the "**Inspectorate**")
A. Juozapavi iaus g. 6 / Slucko g. 2
LT-09310 Vilnius
Lithuania

www.ada.lt

Notification or registration scheme and timing

Unless the processing is exempt, personal data may be processed by automated means subject to notification by the *data controller* or its representative to the Inspectorate before the intended commencement of the data processing activities. Such data processing operations may be carried out only if notification has been filed with the Inspectorate. The Inspectorate has to register the notifications in the public register of Personal Data Controllers and is entitled to require amendments or clarifications in the filing and intended data processing scheme. The Inspectorate may also refuse to register data processing, which it deems improper, or if the *data controller* does not comply with the amendments required by the Inspectorate.

Sensitive data and public data files processed by automated means are subject to prior approval of the Inspectorate. Within one month of receipt of a notification, the Inspectorate must carry out checks according to its procedure and either grant or refuse authorisation.

There is no charge for notification.

Exemptions

Exemptions from notification apply when the data are processed for the purposes of internal administration, when personal data are processed for journalistic purposes or the purposes of artistic or literary expression, or other means of providing information to the public, where non-profit organisations manage data about their members, or data are processed for the purposes of ensuring state and official secrets.

Appointment of a data protection officer

A data protection officer may be appointed in a legal entity which manages the personal data (*data controller*). If no data protection officer is appointed, the CEO of the *data controller* will be responsible for data protection compliance and is also liable for any legal violations of the DPA.

Personal Data

What is personal data?

The definition of personal data in the DPA is based on the *standard definition of personal data*. In particular, it only applies to data pertaining to an identifiable individual. Latest case law and administrative practice in 2012 interpret the definition increasingly broadly. For example, information is treated as personal data if publicly available material can be used to indirectly identify the relevant individual. In particular, the courts and the Inspectorate recognised car license plates and postal addresses (excluding the individual's name) as personal data.

The only notable exception, established through current practice, is the treatment of employee data. Where the public disclosure of that information is necessary for the purposes of employment (e.g. providing remuneration information about on the CEO or contact details for sales representatives), it is not treated as being subject to the protections in the DPA.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the standard conditions are interpreted rather narrowly and to the benefit of the *data subject*.

The legitimate interest exception has been expressly recognised (although available in the DPA since the original legislation) in the ruling by the High Administrative Court of the Republic of Lithuania in Chief Vilnius Police Commissariat v. Data Protection Inspectorate. This related to the online publication of the personal data of individuals convicted for driving under the influence of alcohol, narcotics and similar substances. The court ruled that such publication does not infringe upon personal data protection, as it is justified by the legitimate public interest in prevention of such acts.

The DPA contains limited exemptions for certain types of processing. For example, processing for domestic purposes or manual processing of personal data are largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

There are no special formalities to obtain consent from the *data subjects*, apart from the requirement that consent shall be issued freely and independently. In cases where the relationship between the *data controller* and the *data subject* is subordinate, such as employee *data processing* or consumer data processing, written consent is strongly recommended, as the burden of proof of establishing free and independent consent lies with the employer or business.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) information about previous convictions.

Are there additional rules for processing sensitive personal data?

Processing of sensitive personal data is generally prohibited. Exceptions are allowed if the *standard conditions for processing sensitive personal data* are met. Processing of sensitive personal data for medical treatment is allowed when it is in the vital interests of the *data subject* and he/she is unable to issue consent for such processing due to his/her medical condition. In addition, it is possible to process this data for the prevention and investigation of criminal offences, as well as for litigation purposes.

Are there any formalities to obtain consent to process sensitive personal data?

The *data subject's* consent to the processing of sensitive data must be expressed clearly, in a written or equivalent form or by any other form giving unambiguous evidence of the *data subject's* free will. There are no special requirements to obtaining consent from employees.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. *Data processors* are also regulated by the DPA, although to a much lesser extent. In particular the *data processors* have obligations with respect to disclosing information to the *data subject*, as well as maintaining adequate data security.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to personal data either processed by automated means or by manual means in filling systems (lists, card indexes, files, codes, etc.). A filing system means any structured set of personal data arranged in accordance with specific criteria relating to the person, allowing an easy access to personal data in the file.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation if they suffer damage or damage and distress. The DPA expressly prescribes that damages include both pecuniary loss and non-pecuniary damages. There is no notable case law to date in which a *data subject* has been awarded pecuniary or non-pecuniary loss resulting from the data protection violation.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. *Fair processing information* shall be provided to the *data subject* in cases where the personal data has been obtained from a third party or prior to it being released to a third party.

The DPA expressly requires the provision of information about: (i) sources and/or recipients of the personal data; (ii) purposes of data processing; and (iii) *data subject's* rights. Provision of this information is mandatory. Information must be provided in writing if the *data subject* so requests.

The DPA does not provide any specific requirements regarding the language of the information or reference to data protection legislation. However, information has to be clear and comprehensible to the *data subject*. According to other regulations, all information to consumers must be provided in the national language (Lithuanian).There are no notable cases on the provision of the *fair processing information* in the Lithuanian jurisdiction.

Rights to access information

Data subjects may obtain their *subject access information* upon submitting to the *data controller* or the *data processor* a document certifying their identity. A subject access request shall be satisfied free of charge at least once a year. A follow-up subject access request (after the free annual subject access request is exhausted) may be subject to a fee, which shall not exceed the actual expenses incurred in satisfying such request.

Objection to direct marketing

As a general rule, processing of personal data for the purposes of direct marketing is not allowed without prior consent that expressly refers to the processing of personal data for direct marketing purposes, however, the DPA provides for the *similar products and services exemption*, if marketed to existing customers. Along with the request for consent, the *data subject* must also be informed of his/her right to object to such data processing at any latter time. Upon such objection, the *data controller* shall stop processing data for direct marketing purposes immediately.

Other rights

The *data subject* has the right to demand rectification or destruction of his personal data or restriction of further processing, with the exception of storage, where the data are not processed in compliance with the provisions of the DPA or other legislation. Personal data must be rectified and destroyed in response to the request of the *data subject*, as long as there are no legal grounds to continue the data processing, and on the basis of documents confirming his identity and personal data.

The *data subject* has the right to object to the processing of his personal data. The *data subject* has the right to object to automated decision-making and request manual re-evaluation. The *data subject* has the right to demand written responses from the *data controller* to the enquiries of the *data subject*, which shall be provided within 30 calendar days.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations* and shall disclose the particular means applied to the Inspectorate in the notification filings.

Specific rules governing processing by third party agents (processors)

The *data controller* must choose a *data processor* providing guarantees in respect of adequate technical and organisational data protection measures and ensuring compliance with those measures. The *data controller* must have a written contract with the *data processor* requiring it to comply with the *standard processor obligations* and provide adequate security measures. In addition, the staff processing personal data, when applying for a job or when performing their work, must assume an obligation in writing to keep the personal data confidential when the data are not meant for public disclosure. This obligation remains valid after the employment has ended.

Notice of breach laws

Under the Law on Electronic Communications (the "**LOEC**"), which was originaly adopted on 15 April 2004 (came into force on 1 May 2004) and was most significantly amended on 26 June 2011 (came into force as of 1 August 2011), providers of publicly available electronic communications services must notify the Inspectorate of any personal data breach without undue delay. The provider must also notify the individual of such breach where it is likely to adversely affect their personal data or privacy, unless the provider can demonstrate, to the satisfaction of the Inspectorate, that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. In any case, the Inspectorate may require the provider to notify the individual of the personal data breach.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Personal data can only be transferred outside of the EEA with the authorisation from the Inspectorate unless the *standard conditions for transborder dataflow* are satisfied. Nevertheless, authorisation is still required for transfers based on the *Model Contracts* or to *whitelisted countries*.

Notification and approval of national regulator (including notification of use of Model Contracts)

If the conditions above are not satisfied, personal data may only be transferred to data recipients in foreign countries after receiving authorisation from the Inspectorate.

Such authorisation may be issued provided that there is an adequate level of protection in the recipient country. The Inspectorate may, however, grant authorisation to transfer personal data to a foreign country which does not guarantee an adequate level of protection, if the *data controller* transferring the personal data specifies to the recipient of the data in a contract the requirements for the safeguarding of personal data. In practice an adequate level of protection is assumed in respect of transfers based on the *Model Contracts*, Safe Harbor principles, *binding corporate rules* or to whitelisted countries.

Use of binding corporate rules

The Inspectorate recognises the use of *binding corporate rules* as a means to ensure an adequate level of protection, however it does not provide any exemptions or incentives from the transfer authorisation requirements.

Enforcement

Sanctions

Any act of non-compliance with the DPA or secondary data protection legislation gives rise to civil and administrative (but not criminal) liability. Administrative sanctions include reprimand and monetary fines of amounts from EUR 30 to EUR 1,200.

Recent case law has allowed sanctions under the Law on Advertising to be applied in case of marketing violations affecting personal data. As a result, significantly higher sanctions of up to EUR 9,000 would apply for violation of direct marketing rules.

Administrative prosecution can only be initiated against individuals who have committed a data protection violation, or the officer responsible for data protection issues within the company which has committed the violation. If such an officer does not exist, the CEO of the entity is held responsible for the data protection issues. The company itself may not be subject to administrative prosecution. Typical administrative penalties are fines from 300 to 1,000 Litas (EUR 85 to 300). Penalties are approximately doubled for repeated violations. A notable exception is the liability for violations of direct marketing rules, which separately applies to the company, which committed the violations. A separate penalty of up to EUR 9,000 would apply for such violations under the Law on Advertising. Responsible individual within such company may be held separately responsible and tried under the administrative prosecution rules outlined at the beginning of this paragraph.

The individual affected by the breach of the DPA is also entitled to claim pecuniary and moral damages.

Practice

In 2011, the Inspectorate carried out 43 preventive investigations; investigated 256 complaints of *data subjects*; issued 90 mandatory orders; and adopted 24 statements on administrative offences, 23 of which were later approved by the court. The violations pertaining to personal data processing on the internet are notably increasing and constituted approximately one third of all violations, whilst violations pertaining to direct marketing have decreased.

The most significant penalty levied to date was 2,000 Litas (EUR 600) against the responsible officer of one of the biggest Lithuanian commercial banks, which was found to be repeatedly infringing the personal data treatment regime by collecting excessive data on its clients and by transferring personal data to other entities.

Enforcement authority

The Inspectorate has no power to impose penalties for violations of the DPA, although it is entitled to take enforcement action including carrying out investigations and issuing mandatory orders. Prosecutions for violations of the DPA are brought before the Lithuanian general practice courts and are heard by one judge, who may impose penalties. Decisions of the court may be appealed to the Lithuanian county courts of general competence.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The LOEC fully implemented the *Privacy and Electronic Communications Directive*.

The LOEC was amended on 1 August 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The LOEC does not expressly refer to the use of browser settings as a means to obtain consent. There is an express requirement for consent to be "prior" to the use of a cookie. The Inspectorate is yet to announce how it is going to interpret and implement these new rules. It is expected that a cautious and gradual approach will be taken.

Regulatory guidance on the use of cookies

In 2012 the Inspectorate has published recommendations about the method of consent to the use for cookies. The guidance confirmed that consent can be obtained through pop ups, banners or website registration while relevant settings contained within current browsers are not likely to form a valid consent. According to the guidance, the users must be given a genuine opportunity not to consent. There is no clear guidance on the possibility to obtain an implied consent.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The LOEC prohibits the use of e-mail for advertising purposes without prior and free consent of the addressees. The LOEC is designed to be implemented along with the DPA, which provides that personal data may be processed for the purpose of direct marketing if this purpose is expressly declared during the collection of the data and the *data subject* has given his express consent.

The practice of the Inspectorate suggests that the right of consent must be clearly and separately explained to the *data subject*, and silence (no response) shall not be considered as consent.

Conditions for direct marketing by e-mail to corporate subscribers

The LOEC prohibits the use of e-mail for advertising purposes without prior and free consent of the addressees. The LOEC is designed to be implemented along with the DPA, which provides that personal data may be processed for the purpose of direct marketing if this purpose is expressly declared during the collection of the data and the *data subject* has given his express consent.

The practice of the Inspectorate, suggests that the right of consent must be clearly and separately explained to the *data subject*, and silence (no response) shall not be considered as consent.

Exemptions and other issues

The *similar products and services exemption* is available under the LOEC. Additionally, the LOEC expressly prohibits use of e-mail for advertising purposes when the sender's identity is disguised or a valid e-mail address for the addressee to cancel the sending of such information is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Generally, direct marketing in any form (including direct marketing by telephone) is not allowed without the prior consent of the individuals who are targeted by such direct marketing. There are ongoing deliberations regarding the DPA as to whether calls to randomly chosen individual telephone subscribers are considered direct marketing, whether a deliberate lack of reference to any personal data has any qualifying effects, as well as whether a call requesting the consent of the individual is considered direct marketing. Although the DPA has warned against such direct marketing calls, the ambiguity is only expected to be cleared through case law (which is lacking so far), or an amendment of the DPA, which is overdue.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

As long as no personal data is involved in the direct marketing (for example, where direct marketing is made to the phone numbers of corporate subscribers), it is not subject to prior consent and, therefore, is generally allowed.

Exemptions and other issues

The *similar products and services exemption* is available if marketed to existing customers.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax to individual subscribers is subject to the general direct marketing regulations, i.e. it is not allowed without prior consent of the target individual.

Conditions for direct marketing by fax to corporate subscribers

As long as no personal data is involved in the direct marketing (for example, where direct marketing is made by fax to corporate subscribers), it is not subject to prior consent and, therefore, is generally allowed.

Exemptions and other issues

The *similar products and services exemption* is available if marketed to existing customers.

Luxembourg.

General I Data Protection Laws

National Legislation

General data protection laws

The amended law of 2 August 2002 on the protection of persons with regard to the processing of personal data (the "**DPA**") implemented the *Data Protection Directive*. The law of 27 July 2007 has simplified and amended the DPA.

Entry into force

The DPA entered into force on 1 December 2002.

National Regulatory Authority

Details of the competent national regulatory authority

Commission Nationale pour le Protection des Données (the "**CNPD**").
1, avenue du Rock'n' Roll
L-4361 Esch-sur-Alzette

www.cnpd.lu

Notification or registration scheme and timing

The *data controller* must notify all processing to the CNPD except if the data processing is subject to a legal exemption. A prior authorisation from the CNPD is required in specific cases, for example the processing of certain sensitive data. The notification/authorisation has to be done prior to the processing. Notification/authorisation costs amount to between EUR 50 and EUR 125.

Exemptions

The exemptions from the notification requirement include: (i) the existence of a data protection officer appointed by the *data controller*; (ii) processing for the sole purpose of keeping a register, that is legally introduced for public information purposes and open to consultation by the public or by a person having a legitimate interest; and (iii) processing necessary to acknowledge, exercise or defend a right at law carried out in accordance with the rules governing legal proceedings applicable to civil matters.

The Law of 27 July 2007 has introduced additional conditional exemptions, which include processing carried out for human resources management purposes if such data are not considered to be sensitive data and if they are not used to perform an evaluation of the *data subject*.

The processing by a *data controller* pursuant exclusively to his personal or domestic activities is excluded from the scope of the DPA.

Appointment of a data protection officer

There is an exception to the notification duty to *data controllers* who have designated a data protection officer. Only data protection officers who have been accredited by the CNPD qualify for this exemption.

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is exempted from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

The DPA requires consent to be a free, specific and informed indication of the *data subject's* wish for his personal data to be processed. Therefore, consent may be implied and is not necessarily required to be in writing.

However, for certain processing operations the DPA requires the *data subject's* consent to be express (i.e. the processing of sensitive personal data) or unambiguous (i.e. the transfer of personal data to third countries that do not provide an

adequate level of protection of personal data). In such cases, obtaining written consent from the *data subject* is recommended for evidential purposes.

The CNPD has been reluctant to consider consent by an employee to be valid, as there may be doubts as to whether such consent is freely given by the employee. Furthermore, the consent of employees as a legitimate condition of data processing by the employer is expressly excluded by the DPA in certain circumstances (i.e. supervision in the workplace).

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data include both: (i) the *standard types of sensitive personal data*; and (ii) genetic data. However, additional restrictions apply to the processing of data relating to offences.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. The processing of specific types of sensitive personal data, such as genetic data, is subject to the prior authorisation of the CNPD.

The processing of data relating to offences, criminal convictions or security measures may only be carried out where specifically permitted by statute. For example, an employer may not process excerpts from a (future) employee's criminal records. So far, the CNPD has recognised that such processing is only possible with regard to: (i) the employees of security firms, in relation to cash transportation; and (ii) directors of credit institutions or other professionals of the financial sector.

Are there any formalities to obtain consent to process sensitive personal data?

The position is essentially the same as for the processing of personal data (see above), except that the DPA requires the consent to be express and, therefore, obtaining written consent is recommended.

Scope of Application

What is the territorial scope of application?

The DPA applies to the *standard territorial test*.

Who is subject to data protection legislation?

The DPA applies to *data controllers*. *Data processors* are not subject to the DPA.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to: (i) the processing of data wholly or partly by automatic means; and (ii) the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. Manual records are, therefore, also subject to the DPA and to the same rules and obligations as electronic records.

Rights of Data Subjects

Compensation

Breach of the DPA will provide *data subjects* with a right to compensation.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. They must also inform the *data subject*: (i) if answering the questions is compulsory or voluntary and the possible consequences of failure to answer; (ii) the existence of the right of access to data concerning him; and (iii) the right to rectify them.

There is no obligation in the DPA to provide this information in one of Luxembourg's official languages (Luxembourgish, French, German) and English is widely accepted for fair processing notices. The *data controller* should, however, ensure that the information is provided in a language the *data subject* is familiar with. There is no obligation to refer to the DPA itself in any *fair processing information*.

Rights to access information

Data subjects may obtain their *subject access information* to *data controllers*. This right may be exercised free of charge, at reasonable intervals and without excessive waiting periods. The right may also be exercised by the *data subject's* beneficiaries if they can prove they have a legitimate interest in the information.

Objection to direct marketing

The *data subject* may also object to the processing of his data for direct marketing purposes and he may forbid the *data controller* to disclose his data to third parties or enable his data to be used by third parties for marketing purposes. The *data controller* must inform the *data subject* about this right.

Other rights

The *data subjects* have a right to rectification, but the way to exercise this right is not specified in the DPA. The *data controller* is required to rectify, delete or block data if such data are incomplete or inaccurate.

The *data subject* may object at any time, for compelling and legitimate reasons relating to his special situation, to the processing of any data on him except in cases where legal provisions expressly provide for that processing. Where there is a justified objection, the processing instigated by the *data controller* may not involve those data.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations*. A description of these measures and of any subsequent major change must be communicated to the CNPD at its request, within 15 days.

Specific rules governing processing by third party agents (processors)

If the processing is carried out on behalf of the *data controller*, the *data controller* must choose a *data processor* that provides sufficient guarantees as regards the technical and organisational security measures pertaining to the processing to be carried out. It is up to the *data controller* as well as the *data processor* to ensure that the said measures are respected. Any processing carried out on behalf of a *data controller* must be governed by a written contract or legal instrument binding the *data processor* to the *data controller* and requiring the *data processor* to comply with the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any general obligation to inform the CNPD or *data subjects* of a security breach. However, the *data controller* in certain sectors may be required to inform sector regulators of any breach (for example, financial services firms may be required to inform the financial services regulator of any breach).

Specific notice of breach laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive* which have been implemented into national law by a law dated 28 July 2011.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Data transfers to a third country may take place only where: (i) that country provides an adequate level of protection of personal data and complies with the provisions of the DPA, which includes the *whitelist countries*; or (ii) where the *standard conditions for transborder dataflow* are satisfied. At the request of the CNPD, a report stating the conditions under which the transfer is made has to be provided by the *data controller*.

If the EU Commission or the CNPD finds that a third country does not have an adequate level of protection, transfer of data to that country is prohibited.

Notification and approval of national regulator (including notification of use of Model Contracts)

In the case of a transfer made to a third country that does not offer an adequate level of protection, the CNPD may authorise, as a result of a duly reasoned request, a transfer or set of transfers of data to a third country if the *data controller* offers sufficient guarantees in respect of the protection of the privacy, freedoms and fundamental rights of the *data subjects*, as well as the exercise of the corresponding rights.

These guarantees may result from appropriate contractual clauses. In particular, any transfer based on the *Model Contracts* must be authorised by the CNPD.

Use of binding corporate rules

The CNPD accepts the use of *binding corporate rules* and approved eBay's *binding corporate rules* package. Luxembourg is part of the mutual recognition club for *binding corporate rules*. Data transfers made to a third country that does not offer an adequate level of protection pursuant to *binding corporate rules* still must be approved by the CNPD. Such approval will be automatic in case of mutually recognized *binding corporate rules* already approved by another regulator.

Enforcement

Sanctions

The sanctions for breaching the DPA are both civil and criminal (they range from eight day's to one year's imprisonment and/or a fine between EUR 251 and EUR 125,000). In addition, the CNPD may make administrative disciplinary sanctions. Without prejudice to the criminal sanctions introduced by the DPA and the actions for damages governed by ordinary law, in the event that a processing operation violates the formalities provided for under the DPA being undertaken, any person is entitled to introduce an action for discontinuance of that processing in summary proceedings.

Practice

According to the latest available information, no sanctions have been imposed so far by the CNPD. The District Court of Luxembourg-City has, however, imposed a criminal fine of €7,000 on an employer that unlawfully installed a CCTV system and monitored its employees.

Enforcement authority

The CNPD has the power to investigate and is entitled to engage in legal proceedings in the interests of the DPA. The CNPD will notify the legal authorities (State Prosecutor or President of the District Court) of any offences of which it is aware.

In addition, the CNPD may make administrative disciplinary sanctions. Without prejudice to the criminal sanctions introduced by the DPA and the actions for damages governed by ordinary law, in the event that a processing operation violates the formalities provided for under the DPA being undertaken, any person is entitled to introduce an action for discontinuance of that processing in summary proceedings.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The law of 30 May 2005 relating to specific provisions concerning the processing of personal data and the protection of privacy in the electronic communications sector, modifying provisions 88-2 and 88-4 of the Criminal Instruction Code and modifying the DPA (the "**ECA**"), has implemented Article 13 of the *Privacy and Electronic Communications Directive*.

The ECA was amended on 28 July 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. The ECA expressly refers to the use of browser settings as a means to obtain consent. There is an express requirement for consent to be "prior" to the use of a cookie.

Regulatory guidance on the use of cookies

The CNPD has not yet provided any guidance on the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The ECA provides that sending direct marketing e-mails shall only be permitted with the prior consent of the recipient.

Conditions for direct marketing by e-mail to corporate subscribers

The ECA provides that sending direct marketing e-mails shall only be permitted with the prior consent of the recipient.

Exemptions and other issues

The *similar products and services exemption* applies. The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The ECA provides that sending direct marketing by telephone is only permitted with the prior consent of the *data subject*.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The requirement for consent only applies to individuals. However, it is not permitted to send direct marketing by telephone to corporate subscribers who have previously objected to such telephone calls.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The ECA provides that sending direct marketing faxes is only permitted with the prior written consent of the *data subject*.

Conditions for direct marketing by fax to corporate subscribers

The requirement for consent only applies to individuals. However, it is not permitted to send direct marketing faxes to corporate subscribers who have previously objected to such faxes.

Exemptions and other issues

No exemptions apply.

Malta.

Contributed by Emirates International Telecommunications LLC & Mamo TCV Advocates

General | Data Protection Laws

National Legislation

General data protection laws

The Data Protection Act 2001 (the "**DPA**"), Chapter 440 of the Laws of Malta implemented the *Data Protection Directive*.

Entry into force

The DPA came into force on 15 July 2003, subject to transitional periods for certain provisions. These periods have now expired and both automated and manual processing activities are regulated by all the provisions of the DPA.

National Regulatory Authority

Details of the competent national regulatory authority

Office of the Information and Data Protection Commissioner (the "**Office**")
2, Airways House, Second Floor
High Street
Sliema SLM 1549
Malta

idpc.gov.mt

Notification or registration scheme and timing

Data controllers must notify their processing of personal data to the Office. This involves the filing of information relating to the processing operations carried out by the *data controller*, against payment of a notification fee of EUR 23.29, renewable annually, and the subsequent notification of any updates regarding new processes, prior to implementing such new processes.

Exemptions

By virtue of Legal Notice 162 of 2004, published on 16 April 2004, an exemption from notification has been laid down in circumstances where the only personal data processed by a company are those contained in its Memorandum and Articles of Association as registered with the Registrar of Companies under the Companies Act. Moreover the following categories of persons are obliged to notify but are exempt from payment of the notification fee: (i) self-employed persons who carry on a trade, business, profession or other economic activity and do not employ any employees with them; and (ii) any philanthropic institutions and similar organisations, band clubs, sports clubs and similar institutions, registered trade unions and political parties and clubs adhering to political parties, which are also exempt from tax under the Income Tax Act.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. The Office has not issued guidance on the definition of personal data to date. In all likelihood, it will follow the Article 29 Working Party's *Opinion on Personal Data*.

Is information about legal entities personal data?

No. However, information about sole traders is personal data as they are treated as individuals.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, most *data controllers* are increasingly opting to satisfy the consent condition. However, the legitimate interests condition has been invoked on several occasions.

The DPA contains exemptions for certain types of processing. For example, processing undertaken by a natural person in the course of a purely personal activity is exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

There are no formalities to obtain consent under the DPA to process personal data. Consent can be express, written, oral or implied. However, obtaining consent from employees can be difficult as, in some cases, it may be hard to demonstrate that consent has been freely given by the employee.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data mean the *standard types of sensitive personal data*. Data relating to offences, criminal convictions or security measures may only be processed under the control of a public authority and a complete register of criminal convictions may only be kept under the control of a public authority. Legal Notice 142 of 2004 contains a set of more detailed regulations on the processing of personal data by the police.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met.

Are there any formalities to obtain consent to process sensitive personal data?

Insofar as the explicit consent condition is concerned, while the law does not lay down any requirement for such consent to be given in writing, this is normal practice, and the Office usually requires some written evidence of such consent if this condition is invoked by the *data controller.*

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*. In addition, it applies to the processing of personal data carried out in the context of activities of a Maltese embassy or High Commission abroad.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. *Data processors* are not subject to the DPA.

Are both manual and electronic records subject to data protection legislation?

Yes, the DPA applies to: (i) the processing of personal data, wholly or partly, by automated means; and (ii) such processing other than by automated means, where such personal data form part of a filing system or are intended to form part of a filing system. A "filing system" is defined by the DPA as any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Rights of Data Subjects

Compensation

Data subjects have a right to file a claim for damages against a *data controller* who processes data in contravention of the DPA or regulations made thereunder.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. They must also provide information about: (i) the recipients or categories of recipients of the data; (ii) whether replies to questions are voluntary or obligatory and the consequences of failure to reply; (iii) the existence of the right to access, rectify and, if applicable, erase the data relating to him/her; and (iv) if the data are not collected from the *data subject*, the categories of data processed.

There is no specific obligation in the DPA to provide this information in English and/or Maltese, though it may be difficult to show the information has been fairly provided if it is not in a language that the *data subject* is familiar with. It is common practice for *data controllers* with a largely Maltese clientele to provide *fair processing information* both in English and Maltese (these being the two official languages in Malta). There is no obligation to refer to the DPA itself in any *fair processing information*.

Rights to access information

Data subjects may obtain their *subject access information* by request to *data controllers*. Requests must be made in writing to the *data controller* and signed by the *data subject*. Replies to access requests must be provided by *data controllers* free of charge.

Objection to direct marketing

A *data subject* may request that a *data controller* stop processing his data for direct marketing purposes. The *data controller* is obliged to appropriately inform the *data subject* of his right to oppose, at no cost, such processing for direct marketing purposes. The *data controller* must then cease such processing within a reasonable period.

Other rights

Data subjects have a right to have their data rectified, blocked or erased where the data would not have been processed in accordance with the DPA.

Data subjects also have the right to ask the *data controller* to reconsider any decisions based solely on automated processing (unless such decisions are taken in the course of entering into or performing a contract with the *data subject*, under certain conditions).

Security

Security requirements in order to protect personal data

Data controllers are obliged to comply with the *general data security obligations*. Regard should also be had to the cost of implementing the security measures.

Specific rules governing processing by third party agents (processors)

Data controllers must further ensure that *data processors* can and actually do implement the *general data security obligations*. In addition, the carrying out of processing by way of a *data processor* must be governed by a written agreement binding the *data processor* to the *data controller* and stipulating that the *data processor* must comply with the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any obligation to inform the Office or *data subjects* of a security breach. However, the DPA does provide that the Office is entitled to obtain, on request, information and any documentation in relation to data security. Moreover, *data controllers* in certain sectors may be required to inform sector regulators of any breach (for example, financial services firms may be required to inform the Malta Financial Services Authority of any such breach).

Specific notice of breach laws apply to the electronic communications sector under Legal Notice 239 (as defined below) which implements the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Transfers to a country outside the EU are permitted if the *standard conditions for transborder dataflow* are satisfied.

Notification and approval of national regulator (including notification of use of Model Contracts)

If a transfer does not satisfy the *standard conditions for transborder dataflow*, they must be notified and further approved by the Office as providing an adequate level of data protection. *Data controllers* are required to complete and submit a data transfer form to the Office providing details of any such transfers that they make to third countries.

The DPA permits transfers within the EU. They must, however, be notified to the Office. The Office must also be notified and must grant approval for *transborder dataflows* where the *Model Contracts* are used.

Use of binding corporate rules

The Office has approved the use of *binding corporate rules* in Malta and Malta is a member of the mutual recognition club.

Enforcement

Sanctions

Sanctions under the DPA are both civil and criminal. A *data controller* in breach of the DPA may also be liable to: (i) an administrative fine imposed by the Office; (ii) an order to pay compensation to the aggrieved *data subject* following a successful action for damages by the *data subject*; or (iii) a criminal fine (currently a maximum of EUR 23,293.73) or imprisonment (currently a maximum of six months) or both.

Practice

During 2011 the Office received a total of 56 complaints, the majority of which concerned the processing of personal data without satisfying a processing condition. In the course of investigating complaints, the Office carried out a number of on-site inspections. No financial sanctions have been imposed to date but the Office took all the necessary actions vested in him by law to admonish *data controllers* who were found in breach of the DPA. Over the years the Office has opted for the approach of educating *data controllers* rather than imposing a financial penalty.

Enforcement authority

The Office has the power, in cases where the DPA has been or is about to be violated, to: (i) institute *civil* legal proceedings; (ii) order the rectification, blocking, erasure or destruction of data; (iii) impose a temporary or definitive ban on processing; or (iv) warn or admonish the *data controller*. In certain circumstances, such as where the *data controller* does not implement the security measures required of him by the DPA, the Office may impose an administrative fine. The Office also has the power to refer to the competent public authority any criminal offence encountered in the course of, or by reason of his functions, such authority then being responsible for imposing any criminal penalty contemplated by the DPA (be that a criminal fine, imprisonment or both). An aggrieved *data subject* may, by writ of summons filed in the competent civil court, exercise an action for damages against a *data controller* who processes data in contravention of the DPA. Such action must be commenced within 12 months from the date when the said *data subject* becomes aware or could have become aware of such a contravention, whichever is the earlier.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Article 13 of the *Privacy and Electronic Communications Directive* has been implemented by the Processing of Personal Data (Telecommunications Sector) Regulations 2003 (the "**ECA**") and subsidiary legislation enacted by Legal Notice 16 of 2003 under the DPA. The ECA entered into force on 15 July 2003.

The amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive* have been implemented into Maltese law by Legal Notice 239 of 2011, entitled Processing of Personal Data (Electronic Communications Sector) (Amendment) Regulations 2011 ("**Legal Notice 239**"), which came into force on 1 January 2013.

Cookies

Conditions for use of cookies

Under Legal Notice 239 consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user. Legal Notice 239 does not expressly refer to the use of browser settings as a means to obtain consent.

Regulatory guidance on the use of cookies

No regulatory guidance has to date been published.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The ECA provides that direct marketing e-mail cannot be sent without prior explicit consent of the subscriber in writing.

Conditions for direct marketing by e-mail to corporate subscribers

The ECA provides that direct marketing e-mail cannot be sent without prior explicit consent of the subscriber in writing.

Exemptions and other issues

It is permitted to send e-mail for the purposes of direct marketing if the *similar products and services exemption* applies. The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided. The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

A person who carries out direct marketing by telephone must, at no charge to the subscriber, ensure that any such direct marketing communications are not sent if the said subscriber requests that such communications cease.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

A person who carries out direct marketing by telephone must, at no charge to the subscriber, ensure that any such direct marketing communications are not sent if the said subscriber requests that such communications cease.

Exemptions and other issues

No exemptions apply. The recipient should be told the identity of the person responsible for the direct marketing call.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The ECA provides that direct marketing by fax cannot take place without prior explicit consent of the subscriber in writing.

Conditions for direct marketing by fax to corporate subscribers

The ECA provides that direct marketing by fax cannot take place without prior explicit consent of the subscriber in writing.

Exemptions and other issues

No exemptions apply. The recipient should be told the identity of the person responsible for the direct marketing fax.

Mexico.

Contributed by Ritch Mueller, S.C.

General | Data Protection Laws

National Legislation

General data protection laws

Federal Law for the Protection of Personal Data in the Possession of Private Parties (the "**LFPDPPP**") supplemented by the Rules of the Federal Law for the Protection of Personal Data in the Possession of Private Parties (the "**Regulation**").

Entry into force

The law was published on 5 July 2010 and came into effect on 6 July 2010. The Regulation was published on 21 December 2011 and came into effect on 22 December 2011.

National Regulatory Authority

Details of the competent national regulatory authority

Federal Institute of Access to Information and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos*) (the "**IFAI**").

Av. México # 151
Col. del Carmen
Coyoacán
C.P. 04100
Delegación Coyoacán
México D.F.

http://www.ifai.org.mx/

Notification or registration scheme and timing

Not required.

Exemptions

None.

Appointment of a data protection officer

Not required, though a person or compliance department must be appointed to deal with the exercise of the *data subject's* rights.

Personal Data

What is personal data?

"Personal data" is defined as any information relating to an identified or identifiable individual. However, the Regulation does not apply to information regarding: (i) legal entities; (ii) individuals acting as merchants or professionals; or (iii) basic work related contact details.

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

In order to process personal data, the *data controller* must obtain the consent of the *data subject* through a Privacy Notice. Consent is not required for the processing of personal data when: (i) it is permitted by law; (ii) the personal data has been obtained from public sources; (iii) personal data has been submitted to a dissociation process; (iv) the processing of personal data is made to comply with the obligations deriving from a contract between the *data controller* and the *data subject*; (v) there is an emergency that might harm an individual or his property; (vi) the processing is for healthcare purposes; or (vii) it is provided by a resolution of the competent authority.

The law also has specific provisions governing domestic and international data transfers. Data controllers may transfer personal data if transfers and their specific purposes are provided in the respective privacy notice. *Data controllers* must obtain the *data subject's* consent by such privacy notice except when, *inter alia*: (i) permitted by domestic law or a treaty to which Mexico is a party; (ii) the transfer is made for healthcare purposes; (iii) the transfer is made within the same group of companies operating under the same internal processes and policies; (iv) it is necessary pursuant to a contract entered into, or to be entered into, for the benefit of the *data subject*, by the *data controller* and a third party; or (v) it is necessary to safeguard public interest or for the pursuit of justice.

Under the Regulation, the *data controller* must also take steps to ensure that data is processed in an accountable manner by, amongst other things: (i) developing policies and programmes; (ii) training staff; (iii) auditing compliance; (iv) reviewing new products and services; and (v) implementing security policies.

Are there any formalities to obtain consent to process personal data?

Consent may be express or implied. Express consent may be given verbally, in writing, through an electronic medium, or by unequivocal signs. Implied consent results from non-objection to a privacy notice provided to the *data subject*.

In certain circumstances express consent must be obtained, for example the processing of financial information or sensitive personal data (see below).

Sensitive Personal Data

What is sensitive personal data?

"Sensitive personal data" is personal data that affects the owner's most intimate sphere, or whose improper use could give rise to discrimination or involves a serious risk to the owner; in particular, data is deemed to be sensitive if it could reveal aspects such as racial or ethnic origin, present or future state of health, genetic information, religious, philosophical or moral beliefs, union affiliation, political opinions or sexual orientation.

Are there additional rules for processing sensitive personal data?

For sensitive personal data, the Privacy Notice sent to the *data subject* must expressly indicate the subject matter of the information.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be both express and written, containing the written, electronic or otherwise authenticated signature of the *data subject*.

Scope of Application

What is the territorial scope of application?

The Regulation applies to processing: (i) by an entity with an establishment in Mexico; (ii) outside of Mexico if conducted for *data controller* in Mexico; (iii) where the Regulation is applicable by principles of international law; or (iv) where the *data controller* is based outside of Mexico but uses equipment in Mexico (other than for the purposes of transit).

Who is subject to data protection legislation?

Data protection legislation is applicable to private parties (both individuals and legal entities), except for credit information companies and individuals who collect and store information for personal or domestic use for a non-commercial purpose or without the intent to disclose such information.

Are both manual and electronic records subject to data protection legislation?

Yes.

Rights of Data Subjects

Compensation

No right to compensation.

Fair processing information

The *data controller* must provide a privacy notice to the *data subject* containing: (i) the identity and domicile of the *data controller*; (ii) the purposes of the processing of information; (iii) the options and mediums that the *data controller* offers to limit the use of disclosure of the information; (iv) the transfer of information to be undertaken, if applicable; and (v) the procedure and medium the *data controller* shall use to communicate modifications to the Privacy Notice.

Rights to access information

Owners of personal data have the right to have access to his/her personal information.

Objection to direct marketing

The Federal Law on Consumer Protection grants consumers the right to be free from being contacted in their home, at their job, by email or by any other means to offer goods and/or services. Additionally, subscribers may prohibit companies from disclosing subscribers' information to third parties.

Other rights

An individual may rectify incorrect or incomplete data and additionally may request the cancellation/withholding of its personal data.

An individual also has the right to request the protection of his/her data, the right rectify his/her personal information, the right to have his/her personal information deleted and the right to oppose the use of his/her personal information.

Security

Security requirements in order to protect personal data

It is necessary to establish and maintain physical and technical administrative security measures designed to protect personal data. The Regulation contains detailed security requirements including obligations to carry out a security risk analysis.

Specific rules governing processing by third party agents (processors)

A *data controller* must ensure that there is a written contract (or similar instrument) with any *data processor* that obliges such party to: (i) process personal data only under the *data controller's* instructions; (ii) implement appropriate security measures and ensure personal data is kept confidential; (iii) delete personal data at the end of the relationship, unless required to keep a record of such information by law; and (iv) not disclose personal data unless instructed to do so, to a subcontractor or when required by law.

The Regulations also contain specific provisions applicable to outsourcing and cloud computing.

Notice of breach laws

It is necessary to inform the *data subject* of any security violations so that the *data subject* takes the appropriate measures to protect its personal data. The Regulations set out certain requirements for the content of such notifications.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

There are obligations applicable to both domestic and international transfers (see "*What are the rules for processing personal data?*", above). However, for international transfers, the transferor must also enter into an agreement or legal instrument, or include a clause to establish the same obligations, to ensure that the use of the personal data continues to be subject to the same level of protection.

Notification and approval of national regulator (including notification of use of Model Contracts)

Not necessary.

Use of binding corporate rules

None.

Enforcement

Sanctions

Penalties vary from a warning notice to fines ranging from 100 to 320,000 days of the minimum daily wage in Mexico City to imprisonment ranging from three months to five years.

These penalties may double in the case of sensitive personal data.

Practice

According to the website of the IFAI, there have not been enforcement actions or sanctions since the LFPDPPP and the Regulation came into effect.

Enforcement authority

The IFAI.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

None.

Mexico.

Cookies

Conditions for use of cookies

No.

Regulatory guidance on the use of cookies

No.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The Federal Law on Consumer Protection grants consumers the right to be free from being contacted in their home, at their job, by email or by any other means to offer goods and/or services. Additionally, subscribers may prohibit companies from disclosing their information to third parties.

Conditions for direct marketing by e-mail to corporate subscribers

None.

Exemptions and other issues

None.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The Federal Law on Consumer Protection grants consumers the right to be free from being contacted in their home, at their job, by email or by any other means to offer goods and/or services. Additionally, subscribers may prohibit companies from disclosing their information to third parties.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

None.

Exemptions and other issues

None.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The Federal Law on Consumer Protection grants consumers the right to be free from being contacted in their home, at their job, by email or by any other means to offer goods and/or services. Additionally, subscribers may prohibit companies from disclosing their information to third parties.

Conditions for direct marketing by fax to corporate subscribers

None.

Exemptions and other issues

None.

The Netherlands.

General I Data Protection Laws

National Legislation

General data protection laws

The general data protection law is the *Wet bescherming persoonsgegevens*, the Data Protection Act ("**DPA**"). The DPA is the basis for secondary legislation, most notably the Exemption Decree DPA (Vrijstellingsbesluit Wbp) which exempts the processing of a range of data categories from the obligation of advance notification ("**Decree**").

Entry into force

1 September 2001.

National Regulatory Authority

Details of the competent national regulatory authority

Dutch Data Protection Authority (*College bescherming persoonsgegevens*) ("**CBP**")

Mailing address:	College bescherming persoonsgegevens Postbus 93374 2509 AJ Den Haag The Netherlands
Visiting address:	Juliana van Stolberglaan 4-10 2595 CL DEN HAAG The Netherlands

www.cbpweb.nl

Notification or registration scheme and timing

The DPA requires advance notification (i.e. prior to commencing processing activities) of processing of data with the CBP (or with the data protection officer, see below) if this processing is fully or partially automated. Such notification can be made electronically or manually via forms made available by the CBP on its website. Registration is free of charge. Although the CBP reviews the registration and may comment on it if sees reason to do so, once registration is made, processing may commence without approval of the CBP being required. All registrations are published at the website of the CBP.

Exemptions

The Decree exempts the processing (not including export of data to countries without adequate protection) of a range of categories of data from the registration obligation (e.g. administration of employees, subscribers, debtors and creditors, clients). The data categories, the purpose for which they are to be processed, the *data subjects* and the retention periods are described in detail and the exemption only applies to the extent that the processing remains within the limits of the description of the Decree. The processing remains fully subject to the requirements of the DPA; the Decree only provides an exemption to the notification obligation. Moreover, the exemption only applies to the processing by a single *data controller*.

Appointment of a data protection officer

There is no legal obligation to appoint a data protection officer. However, the appointment of a data protection officer can avoid the need to notify the CBP of new processing (see above).

Personal Data

What is personal data?

The DPA defines personal data in line with the *standard definition of personal data* as any information relating to an identified or identifiable natural person.

Is information about legal entities personal data?

The DPA defines personal data as data related to natural persons and therefore does not directly apply to information about legal entities (i.e. entities with legal personality as opposed to e.g. partnerships). Nevertheless, the definition of personal data is very broad and may also apply where the combination of information about legal entities with other data may determine how a natural person is assessed or treated. A recent interim relief judgment of the Amsterdam District Court in a case against Google indicates that the fact that the trade of a legal entity (which was visible in a Google Street View picture) includes the name of a natural person is as such insufficient to qualify that trade name as "personal data".

What are the rules for processing personal data?

The DPA essentially follows the *standard conditions for processing personal data*. In practice, the legitimate interests condition is frequently relied upon as ground for processing non-sensitive personal data.

Processing for personal and domestic purposes is excluded. Processing for exclusively journalistic, artistic or literary purposes is excluded as well but remains subject to certain obligations with regard to processing, security, the position of *data controllers* and liability vis-a-vis *data subjects*.

Are there any formalities to obtain consent to process personal data?

No formalities apply. Consent can be given in any form.

Sensitive Personal Data

What is sensitive personal data?

The DPA contains a stricter regime for a specified category of data (often referred to as "special" or "sensitive" personal data, although the DPA does not use these terms), which comprises personal data on a person's religion, race, political views, health, sexuality, trade union membership, i.e. the *standard types of sensitive personal data*.

However, this stricter regime also applies to: (a) criminal behaviour and personal data on unlawful or objectionable behaviour in relation to an injunction imposed with regard to such behaviour; and (b) "indirect" sensitive data, i.e. personal data that is as such not sensitive but from which sensitive characteristics can be derived, e.g. a photo or address list from a religious organisation from which information on racial origin or religious beliefs can be derived.

Are there additional rules for processing sensitive personal data?

Under the DPA the starting point is a prohibition on the processing of sensitive personal data. To this prohibition a number of exemptions apply, both specific exemptions for specific types of sensitive personal data as well as a number of general exemptions i.e. (i) explicit consent of the *data subject*, (ii) where the data has clearly been made public by the *data subject*, (iii) if necessary for the determination, exercise or defence of a right in legal proceedings, (iv) if necessary to protect vital interests of the *data subject* or a third party and it turns out to be impossible to ask for explicit consent, (v) if it is necessary to comply with an obligation under international public law, and (vi) where the law or an individual exemption of the CBP allows this where necessary in view of an important general interest and provided appropriate safeguards apply.

Are there any formalities to obtain consent to process sensitive personal data?

Such consent must be explicit but otherwise no formalities apply, e.g. written consent is not required.

Scope of Application

What is the territorial scope of application?

The *standard territorial test* is applicable under the DPA.

Who is subject to data protection legislation?

The DPA primarily applies to and imposes restrictions and obligations on *data controllers*. Nevertheless, the DPA provides that the *data processor* is liable vis-a-vis the *data subject* where its activities result in infringements of the DPA and damages, and requires the *data processor* to ensure the confidentiality of the data.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to the fully or partly automated processing of personal data. The DPA also applies to non-automated processing of personal data, but only to the extent this personal data is (or is intended to be) contained in a "file", i.e. a structured collection of personal data that is accessible according to certain criteria and relates to different individuals, regardless of whether such collection is centrally stored or functionally or geographically spread.

Rights of Data Subjects

Compensation

The DPA provides for a right to compensation for *data subjects* where they suffer damages as a consequence of the infringement by the *data controller* or the *data processor* of the DPA or secondary legislation based on the DPA.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects* prior to obtaining the personal data from them or from third parties, unless this information is already known to the *data subject*. If the personal data has been obtained from a third party and providing the *fair processing information* would be impossible or take a disproportionate effort or is required by law, this obligation does not apply.

Part of the *fair processing information* is any further information in so far as such further information is necessary, having regard to the circumstances in which the data is collected, to guarantee fair processing. This may vary from case to case. The legislative history of the DPA mentions as an example the situation whereby certain questions are posed in the process of entering into a contract (e.g. via a standard form) and part of the information requested is not necessary for the contract (e.g. general statistical information); this should be indicated. Another example is that of a significant change in the processing, e.g. in case there will be other recipients than those initially envisaged.

Rights to access information

Data subjects may obtain their *subject access information* by request to *data controllers*. The costs may not exceed €5. The DPA provides that in response to such a request the *data controller* must provide a "complete overview in understandable form" of such data, which, according to the broad interpretation of the Dutch Supreme Court (in the 2007 Dexia cases), will usually (but not always) entail an obligation for the *data controller* to provide the *data subject* with copies of all relevant documents.

Objection to direct marketing

A *data subject* may require that a *data controller* stop processing his personal data for direct marketing purposes. The *data controller* must then cease such processing immediately.

Other rights

Data subjects may ask the *data controller* to correct, supplement, delete or block the data processed about them in the event that such data is inaccurate, incomplete or irrelevant for the purposes of the processing, or is being processed in any other way that infringes a legal provision. They will have to specify the changes in their request.

The DPA prohibits, subject to certain exceptions decisions about a *data subject* based solely on automatic processing aimed at obtaining a picture of certain aspects of his personality (i.e. profiling); to the extent such decisions are allowed (e.g. if related to the performance of a contract), the *data controller* must provide the logic underlying such processing.

Security

Security requirements in order to protect personal data

The DPA requires the *data controller* to implement the *general data security obligations*. The *data controller* may, in deciding the appropriate level of security, take into account not only the state of the art but also the costs of implementation.

Specific rules governing processing by third party agents (processors)

The processing of personal data by a *data processor* must be in accordance with a written contract containing *the standard processor obligations* and the *data controller* is required to supervise compliance with these obligations, e.g. via contractually agreed audits.

Notice of breach laws

As of 5 June 2012 the *Citizens' Rights Directive* has been implemented into the Telecommunications Act, which now requires providers of public electronic communications networks and services to immediately notify OPTA (as of 1 April 2013 the ACM)(as defined below) of a breach of security that is detrimental to the protection of personal data that is processed in connection with the supply of a public electronic communications service in the European Union. The *data subject* must be immediately notified as well in case the breach will likely have negative consequences for his privacy. A specific website has been made available for notifications (www.meldplichttelecomwet.nl).

On 5 March 2013, a legislative proposal to introduce a general obligation to notify the CBP of data leaks has been submitted to the Council of State for advice and will subsequently be submitted to parliament (and will become public from that moment). A draft which was published in December 2011 for consultation contained an obligation for *data controllers* to notify the CBP and *data subjects* immediately of breaches of security that are reasonably likely to result in unlawful processing and damage to personal data and the privacy of *data subjects*.

The CBP published on 1 March 2013 detailed policy guidelines that set out its interpretation of what it considers to be "appropriate" data security measures.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Under the DPA *transborder dataflows* may take place where they satisfy the *standard conditions for transborder dataflow*. Where consent of the *data subject* is relied on, this consent should be unambiguous.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no obligation to notify the CBP of any *transborder dataflow* that satisfies the standard conditions for *transborder dataflow*. Where these conditions are not met, an individual licence must be obtained.

Use of binding corporate rules

Binding corporate rules are accepted in The Netherlands and it is a member of the mutual recognition club. Recent approvals include Schlumberger, Sara Lee, Royal Philips Electronics, ABN AMRO, Koninklijke DSM and ING Bank.

Enforcement

Sanctions

The CBP may impose an administrative fine not exceeding € 4,500 on *data controllers* for infringements in relation to the notification obligation, including non-notification, commencing of *data processing* prior to notification, incomplete notification and failure to inform the CBP of amendments.

The CBP may also impose an enforcement order to remediate non-compliance. Failure to comply with that enforcement order may either result in the CBP being authorised to remediate the non-compliance itself or to impose a single or periodical penalty fine, the level of which is at the discretion of the CBP but must be reasonably proportional.

Moreover, the infringement of notification obligations may qualify as criminal violation, subject to penalty fines not exceeding € 3,900 where the violation is committed negligently and €19,500 or up to six months imprisonment in case of intentional infringement. Where the *data controller* is a legal entity, these amounts may be increased to € 7,800 and € 78,000 respectively in case the court finds this a more appropriate amount in the circumstances at hand.

The CBP is empowered to investigate, either upon request of an interested party or on its own motion, compliance with the provisions of the DPA, including privacy audits. The CBP regularly initiates such investigations and publishes the results.

Practice

In 2011, the CBP conducted 85 investigations on its own motion and dealt with 129 complaints. The CBP considers the investigations on its own motion an important and effective instrument to ensure general compliance and awareness and therefore dedicates a significant amount of its limited resources to such labour intensive investigations. The CBP issued six enforcement orders in 2011 (a significant decrease compared to 2009 (26 enforcement orders) and 2010 (35 enforcement orders)) and, similarly to 2009 and 2010, imposed no administrative fines. The CBP regularly publishes guidelines and opinions on current matters. In prioritising its investigational capacities, the CBP gives priority to (suspected) serious and structural infringements that affect many people and where CBP enforcement can make a real difference. The CBP paid specific attention to, among other topics, profiling, data leaks, security of medical data, cloud computing and international cooperation (the CBP is currently chairing the Article 29 Working Group).

OPTA (as of 1 April 2013 the ACM) is actively enforcing the ePrivacy provisions of the Telecommunications Act. In 2011 OPTA imposed over € 1 million in administrative fines for infringement of the provisions on telemarketing as well as significant fines and enforcement orders for sending spam (i.e. unsolicited automated communication by e-mail, fax or SMS). In December 2012 OPTA imposed a total amount of € 845,000 in fines on a number of lotteries for infringement of the telemarketing provisions.

Enforcement authority

Administrative fines and measures can be imposed by the CBP itself. Criminal sanctions are imposed by the Dutch criminal court following prosecution by the Office of the Public Prosecutor (openbaar ministerie). Interested parties (e.g. *data subjects* claiming to have suffered damages as a consequence of infringements of the DPA) may initiate proceedings in the civil courts, either on the merits or in summary proceedings. OPTA (as of 1 April 2013 the ACM) has the authority to impose fines and enforcement orders with regard to the provisions that it enforces, and can impose significantly higher fines than the CBP (up to €450,000).

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

As of 5 June 2012, the Telecommunications Act implements the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. These provisions are currently enforced by the Independent Post and Telecoms Authority ("**OPTA**") and, as of 1 April 2013, the Authority for Consumer and Market ("**ACM**").

Cookies

Conditions for use of cookies

The Telecommunications Act provides that cookies may only be placed where (a) clear and complete information on the use of cookies, in any event indicating their purpose, has been provided and (b) consent for the use of cookies has been

obtained. The legislator did not provide further guidance as to how consent is to be obtained, although it is clear that such consent must be free, specific and informed (based on specific information, not a general reference to terms and conditions or a privacy statement), and that it must be given before the cookie is placed.

The strict requirements on advance information and consent do not apply where cookies are only intended for carrying out the communication over a network or the provision of an explicitly requested service. This exception is narrowly construed and for example does not cover analytical cookies.

Moreover, the Telecommunications Act contains as of 1 January 2013 a legal presumption to the effect that tracking cookies constitute the processing of personal data and are therefore subject to the rules of the DPA, unless the user of tracking cookies can demonstrate that no personal data is being processed.

In December 2012 the Minister of Economic Affairs announced that he will look into the possibility of exempting first party anonymous analytical cookies from the prior consent requirement (but not third party analytical cookies). In March 2013, it appeared that a majority of the lower house is in favour of such an exemption, as well as the possibility of accepting implied consent in stead of explicit consent in certain cases. The Dutch cookie legislation, which has proven to be highly controversial so far, is likely to remain work in progress for the time being.

Regulatory guidance on the use of cookies

Upon their entry into force on 5 June 2012, the information and consent requirements for cookies have proven to be highly controversial and have been severely criticised. The law imposes strict rules, but leaves important elements open, e.g. how exactly consent can be obtained in a compliant manner, resulting in a broad range of different approaches by websites. The law has also been criticised for being overly broad in scope, and for imposing onerous requirements in situations where no, or no significant threats to privacy of users are likely.

OPTA has engaged in discussions with market operators on the interpretation of the rules. Its most recent interpretation of the rules was published in February 2013..

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The Telecommunications Act prohibits unsolicited communication by e-mail (as well as faxes and automated communication systems) for commercial, non-commercial or charitable purposes, unless the sender can demonstrate prior consent of the subscriber. The identity of the sender, an opt-out address and e-commerce information must be provided.

Conditions for direct marketing by e-mail to corporate subscribers

The provisions on unsolicited communication via e-mail also apply to corporate subscribers.

Exemptions and other issues

No prior consent is required for unsolicited electronic messages to corporate subscribers (legal entities or individuals acting in a commercial capacity) if contact details are used that were published and designated by the subscriber for that purpose, or where the subscriber is established in a country outside the EEA and the local rules on unsolicited communication are complied with.

The recipients of electronic contact details may use those details to transmit communications for commercial, non-commercial or charitable purposes where the *similar products and services exemption* applies.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The Telecommunications Act has a separate regime for unsolicited communication for commercial, non-commercial or charitable purposes by telephone. In principle, such communication is allowed, but subscribers may opt out.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The regime with regard to unsolicited communication via telephone does not apply to corporate subscribers but only to natural persons.

Exemptions and other issues

There is no prescribed form for opting out, but an important method is provided via a special register (colloquially referred to as the "bel-me-niet-register" or "do-not-call-me-register") that is kept by an independent third party and which contains the contact details of subscribers who formalise their objection to being called by inclusion in the register. In individual calls subscribers should be reminded of the register and be offered the possibility to object to further use of their electronic contact details and to be included immediately in the register.

The restrictions on unsolicited commercial communications do not apply where the contact details have been obtained in connection with a sale of a product or service or a donation to a charity, and these contact details are used for direct marketing of own similar products or donations to the same non-commercial or charitable organisation.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The Telecommunications Act prohibits unsolicited communication by fax for commercial, non-commercial or charitable purposes, unless the sender can demonstrate prior consent of the subscriber.

Conditions for direct marketing by fax to corporate subscribers

The provisions on unsolicited communication via fax also apply to corporate subscribers.

Exemptions and other issues

There are no exemptions.

Norway.

Contributed by Advokatfirma Wiersholm AS

General I Data Protection Laws

National Legislation

General data protection laws

The *Data Protection Directive* has been implemented by the Personal Data Act (the "**DPA**") dated 14 April 2000. The DPA was last amended 20 April 2012 to include regulations protecting children's privacy, and to revise the regulations on video surveillance. The DPA is supplemented by the Personal Data Regulation (the "**Regulation**") dated 15 December 2000, as last amended on 7 May 2010.

Entry into force

Both the DPA and the Regulation came into force on 1 January 2001.

National Regulatory Authority

Details of the competent national regulatory authority

The Data Protection Authority (the "**Authority**")
P.O. Box 8177
Dep, N-0034
Oslo
Norway

www.datatilsynet.no

Notification or registration scheme and timing

The *data controller* must notify the Authority before processing personal data by automatic means or establishing a manual personal data filing system which contains sensitive personal data. The notification must be made no later than 30 days prior to commencement of processing and is free. The DPA merely establishes an obligation to notify, and the prior approval of the Authority is not required.

The processing of sensitive data and the processing of personal data in the telecommunications sector, insurance industry, banks and financial institutions and credit information agencies requires a licence from the Authority prior to processing. There is no charge for a licence.

Exemptions

There are various exemptions from the notification/licensing requirements, i.e. with regard to processing of data as part of administration, and performance of, contractual obligations to customers, subscribers and suppliers and with regard to certain processing of employee data. The appointment of a data protection officer provides an exemption from the obligation to notify, if that officer is approved by the Authority.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer. However, doing so can provide an exemption from the notification duty (see above).

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. Personal data is defined as any information or opinion that may be linked to a natural person.

Is information about legal entities personal data?

Generally, information about legal entities is not regarded as personal data. However, the DPA applies to both individuals and legal persons in relation to credit information agencies.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the legitimate interests condition is frequently relied upon as grounds for processing non-sensitive personal data.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

Consent must be specific, informed and given freely, but need not be in writing. The requirement that consent must be a specific declaration by the *data subject* means that an implied consent will not be valid under the DPA. Obtaining consent from employees can be difficult due to the fact that it can be hard to demonstrate that the consent has been given freely by the employee.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act. Other types of personal data may also be considered sensitive upon an assessment of the character of the data, such as information relating to the *data subject's* economic situation and detailed information which may infringe the *data subject's* privacy if processed.

National identity numbers and video surveillance are not classified as sensitive personal data but are subject to additional processing requirements (set out below).

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. Sensitive data may also be processed if the processing is laid down by law or if processing is necessary for historical, statistical or scientific purposes and the public interest in such processing clearly exceeds the disadvantages it might entail for the *data subject*. In addition, as set out above, a licence from the Authority is required prior to the processing of sensitive data, provided that no exemptions apply.

National identity numbers and other clear means of identification, including biometric data, may only be used in the processing when there is an objective need for certain identification and the method is necessary to achieve such identification.

Video surveillance of a place which is regularly frequented by a limited group of people is only permitted if there is a special need for such surveillance and it must be notified by clear means.

Are there any formalities to obtain consent to process sensitive personal data?

The position is the same as for obtaining consent to the processing of personal data (see above).

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. Only the *general data security obligations* also apply to *data processors*.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to both personal data: (i) processed partly or solely by automatic equipment; (ii) processed otherwise and filed in a personal record system or collected with the intention of being filed in a personal record system; and (iii) all methods of camera surveillance.

Rights of Data Subjects

Compensation

Under the DPA, the *data controller* must compensate for damage suffered if personal data have been processed contrary to the DPA, unless it is established that the damage is not due to error or negligence on the part of the *data controller*. The compensation must be equivalent to the financial loss incurred by the claimant as a result of the unlawful processing. The *data controller* may also be ordered to pay such compensation for damage of a non-economic nature (compensation for non-pecuniary damage) as seems reasonable.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. This also includes: (i) the categories of recipients of data; (ii) the fact that the provision of data is voluntary; and (iii) the existence of the right to access and to rectify the data concerning him.

When a *data controller* or *data processor* contacts the *data subject* or makes decisions to which the *data subject* is subject on the basis of personal profiles, the *data controller* shall inform the *data subject* of: (i) the identity of the *data controller*; (ii) the categories of data which are being used; and (iii) the sources of the data.

There are no requirements as to the form in which the information must be provided but the information shall, upon request, be provided in writing. There are no explicit requirements as to language. However, in some cases the *data controller* may need to provide information in Norwegian in order for the processing to be fair. Further, if processing is based on the *data subjects'* consent, information may need to be in Norwegian in order to obtain an informed consent from the *data subject*.

Rights to access information

Any person may obtain information as regards a specific type of processing: (i) the identity of the *data controller* and of his representative, if any; (ii) who has the day-to-day responsibility for fulfilling the obligations of the *data controller*; (iii) the purpose of the processing; (iv) descriptions of the categories of personal data that are processed; (v) the sources of the data; and (vi) whether the personal data will be disclosed and, if so, the identity of the recipient.

The *data subjects* may obtain their *subject access information* by request to *data controllers*. Before providing access to data relating to a *data subject*, the *data controller* may require that the *data subject* furnish a written, signed request.

The *data controller* shall respond to requests without undue delay and not later than within 30 days. There is no charge for making requests.

Objection to direct marketing

A *data subject* may require that a *data controller* stops processing his personal data for direct marketing purposes and that he is included in the *data controller's* marketing suppression register. Alternatively, the individual may register in a central marketing suppression register. *Data controllers* shall update their register of addresses to reflect the central marketing suppression register prior to sending out marketing for the first time and monthly when the marketing is carried out.

The provisions regarding objection to direct marketing are now implemented in the new Marketing Control Act (see below).

Other rights

The *data subject* has a right to require rectification of personal data which are inaccurate, incomplete or the processing of which is not authorised.

In certain cases, a *data subject* may object to decisions being taken about him based solely on automatic processing.

Security

Security requirements in order to protect personal data

In accordance with the DPA and the Regulation, the *data controller* must, by means of planned, systematic measures, ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data, as well as internal control. The data system and the security measures must be documented, and must be accessible to such employees of the *data controller* that need this in their work, as well as to the Authority and the Privacy Appeals Board.

Specific rules governing processing by third party agents (processors)

Under the DPA, there must be a written agreement between the *data processor* and the *data controller* regarding such processing of information requiring the *data processor* to comply with the *standard processor obligations*.

Notice of breach laws

The Authority must be notified if breach of these security obligations has resulted in the unauthorised disclosure of confidential personal data.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the *standard conditions for transborder dataflow*. Alternatively, the *data controller* can rely on its own assessment of whether the personal data will be adequately protected after they have been transferred outside of the EEA.

In addition, the Authority may allow a transfer even if the above conditions are not fulfilled if the *data controller* provides adequate safeguards with respect to the protection of the rights of the *data subject*. The Authority may stipulate conditions for the transfer.

Notification and approval of national regulator (including notification of use of Model Contracts)

Transborder dataflow does not require notification or approval as such. However, *transborder dataflow* based on *Model Contracts* or *binding corporate rules* is subject to prior approval by the Authority.

Use of binding corporate rules

Transborder dataflow may be based on *binding corporate rules* based on the Authority's specific approval.

Enforcement

Sanctions

Anyone who wilfully or through gross negligence does not comply with the provisions of the DPA shall be liable to fines or imprisonment for a term not exceeding one year, or both. In particularly aggravating circumstances, a sentence of imprisonment for a term not exceeding three years may be imposed.

A coercive fine, which is an administrative sanction, may also be imposed by the Authority.

Practice

In 2011 the Authority carried out 38 investigations in ten different business sectors. Fewer investigations were conducted compared to previous years due to a prioritisation of planning work by the Authority. The Authority also sent out decision letters to 56 municipalities and made 71 individual decisions, of which 6 were characterised as serious.

Based on information that is currently accessible, 55 investigations were carried out in 2012.

The Authority also reviewed the use of cloud computing services last year. The Authority previously indicated that such services do not comply with data protection and privacy requirements. After a lengthy review, the Authority concluded that the use of Google Apps and Microsoft Office 365 cloud services by two municipalities may be compliant with the legal requirements for data protection and privacy, provided that certain conditions are met.

Since the beginning of October 2011 there have been 23 appeals to the Privacy Appeals Board concerning the DPA. Processing in breach of the DPA was established in some of them. In at least five of the decisions by the Privacy Appeals Board the respondent had to adjust his/her practice in order to be in compliance with the DPA.

Since October 2011 there has only been one High Court case and no Court of Appeal decisions related to the DPA.

Enforcement authority

The Authority may issue orders to the effect that the processing of personal data which is contrary to the DPA or the Regulation shall cease or impose conditions which must be fulfilled in order for the processing to be in compliance with the DPA or the Regulation. The Authority may impose a coercive fine (an administrative sanction) which runs from the expiry of the time limit set for the compliance with the order. Decisions by the Authority may be appealed to the Privacy Appeal Board.

The Authority has the power to impose fines for infringement of the DPA following recent changes to the DPA. Prosecutions for criminal offences are brought before the courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Marketing Control Act, dated 9 January 2009 implemented, Article 13 of the *Privacy and Electronic Communications Directive*. The Marketing Control Act came in to force on 1 June 2009. Please note that the Act has introduced provisions which give the Consumer Ombudsman the right to impose fines for infringements of the Marketing Control Act.

The Marketing Control Act, the Ecommerce Act and/or the Ecommerce Regulation have not yet been amended to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. The time limit set for the implementation of the Directive was 25 May 2011. However, the implementation into Norwegian legislation has been delayed. At the time of writing the bill is being considered by the Norwegian parliament and is expected to enter into force in July 2013.

Cookies

Conditions for use of cookies

Currently, pursuant to the Ecommerce Regulation, it is only necessary to inform users of the use of cookies and offer them the right to refuse their use. However, when the Marketing Control Act, the Ecommerce Act and/or the Ecommerce

Regulation is amended to implement the *Citizens' Rights Directive* it will most likely be necessary to obtain consent to the use of cookies, unless the cookie is strictly necessary for the provision of a service to that subscriber or user.

Regulatory guidance on the use of cookies

There is no regulatory guidance on the use of cookies under Norwegian law.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Section 15 of the Marketing Control Act prohibits direct marketing to individuals in the course of business using methods of telecommunication which permit individual communication, such as e-mail, text messaging services to mobile telephones, facsimile or automatic calling machines, without the prior consent of the recipient, unless there is an existing customer relationship and the e-mail is collected in connection with such relationship. A valid consent must be obtained by means of opt-in (a positive indication that the consumer would like to receive marketing, typically by actively ticking a box) rather than opt-out (an opportunity to object to receive marketing). Prior to giving its consent, the consumer must be clearly informed of the extent and contents of the marketing, including how often marketing communications will be sent, which products will be marketed and specific information as to who the marketing communications will be sent from or on behalf of.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing by e-mail to corporate subscribers is permitted provided that the e-mail is sent: (i) to the corporation as such; or (ii) to a relevant contact person within the corporation and the service or product marketed is relevant to the business.

For other types of direct marketing to corporate e-mail addresses, the same conditions apply as for direct marketing by e-mail to individual subscribers.

Exemptions and other issues

Direct marketing using telecommunication such as e-mail is permitted if the *similar products and services exemption* applies. Individual-to-individual e-mail routines set up by companies on the company's website (tip-a-friend) are permitted in most circumstances. An easy means of opt out shall be provided in each individual communication, regardless of the legal grounds on which the direct marketing is based. The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing orally by telephone to individuals does not require prior consent.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Marketing by telephone to corporate subscribers does not require prior consent.

Exemptions and other issues

Section 12 of the Marketing Control Act prohibits direct marketing to individuals by telephone or addressed mail if the individual has chosen to register in the central marketing exclusion register or in the marketer's register of addresses. However, the *similar products and services exemption* applies. Direct marketing by text messaging services is prohibited without the prior consent of the recipient (see above under "Marketing by E-mail").

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Section 15 of the Marketing Control Act prohibits direct marketing to individuals in the course of business using fax without the prior consent of the recipient.

Conditions for direct marketing by fax to corporate subscribers

Direct marketing by fax to corporate subscribers does not require prior consent.

Exemptions and other issues

Direct marketing using a method of telecommunication such as fax is permitted if the *similar products and services exemption* applies. An easy means of opt-out shall be provided.

People's Republic of China.

General | Data Protection Laws

National Legislation

General data protection laws

There is currently no comprehensive legislation that focuses exclusively on the regulation of personal data protection at the national level in China. Instead, there are principles and rules relating to data protection that can be found in various laws, regulations and local provisions, including: (i) general principles relating to privacy in the Chinese Constitution, the General Rules of Civil Law and the Tort Liability Law; (ii) sector-specific provisions, such as laws and regulations relating to the credit reference, Internet, financial, telecommunications, and consumer protection sectors; (iii) legislation in connection with personal data protection at the local level, such as the Shanghai Consumer Protection Rules and the Jiangsu Information Ordinance; and (iv) the Chinese Criminal Law (together, the "**Personal Data Protection Regulations**").

There are also new national guidelines on personal data (the "**Personal Data Protection Guidelines**") issued in 2013 by the Ministry of Industry and Information Technology (the "**MIIT**"). The Personal Data Protection Guidelines are not mandatory regulations or rules but rather are non-binding technical guidelines relating to the collection, use and disclosure of personal data by organisations (other than governmental authories) through information systems.

References to China in this summary are references to the People's Republic of China excluding Taiwan and the Hong Kong and Macau Special Administrative Regions.

Entry into force

The Personal Data Protection Regulations have varying dates on which they entered into force, although note that the key regulations relating to data protection in the credit reference industry become effective on 15 March 2013.

The Personal Data Protection Guidelines became effective on 1 February 2013.

National Regulatory Authority

Details of the competent national regulatory authority

There is no specific national regulatory authority. Instead, competent authorities in some industries monitor the enforcement of the Personal Data Protection Regulations in their respective areas. For example, the MIIT takes charge of implementing the Personal Data Protection Regulations in the telecommunications and Internet sectors while the People's Bank of China takes charge of implementing the Personal Data Protection Regulations relating to the credit reference and financial sectors.

Notification or registration scheme and timing

There are no rules requiring the notification or registration of the collection of personal data.

Exemptions

Not applicable.

Appointment of a data protection officer

The Personal Data Protection Regulations do not require the appointment of a data protection officer.

The Personal Data Protection Guidelines state that the administrator of personal data should appoint a specific data protection officer or department to be in charge of the protection of personal data.

Personal Data

What is personal data?

There is no uniform definition of personal data in the Personal Data Protection Regulations. The scope of personal data is defined differently amongst the various Personal Data Protection Regulations. Although there is no unified definition, generally any information that relates to an individual which by itself or in combination with other information could disclose the identity of that individual can be regarded as personal data. This is similar to the *standard definition of personal data*.

The Personal Data Protection Guidelines include a similar definition of personal data. In addition, the Personal Data Protection Guidelines classify personal data into two catogories: general personal data and sensitive personal data. General personal data includes all personal data other than sensitive personal data.

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

There are no uniform rules for processing personal data in the Personal Data Protection Regulations. However, the Personal Data Protection Regulations include rules on the processing of personal data in certain sectors. For example, in the banking sector, informed consent must be obtained from a *data subject* before his or her personal data is provided to a *data processor*. In the telecoms sector, internet companies must: (i) obtain the prior consent of the *data subject* before collecting and using their personal information; (ii) maintain collected data confidentiality; and (iii) not divulge, misuse, alter or sell such information or provide such information to other parties illegally. In the credit reference sector, the written consent of a *data subject* is required if a third party asks for personal data of that *data subject* from a credit reference agency.

The Personal Data Protection Guidelines include guidance on how organisations should process personal data. For example, the Personal Data Protection Guidelines state that the expressed or tacit consent of a *data subject* must be obtained before processing personal data. When collecting general personal data, a *data subject's* tacit consent can be deemed to be given. However, an organisation must cease collecting general personal data, or delete personal data already collected, if the *data subject* has explicitly rejected such collection. Before collecting personal data, an organisation must clearly inform the *data subject* about the purpose and method of collection, as well as the measures that the organisation will take to protect the personal data and the complaints channels open to the *data subject* to deal with issues relating to the organisation's use of the personal data. In addition, an organisation may not generally disclose personal data to any individual, organisation or institution if that disclosure is not relevant to the purpose of collection or without the *data subject's* consent.

Are there any formalities to obtain consent to process personal data?

There are no uniform formalities in the Personal Data Protection Regulations. However, the Personal Data Protection Regulations relating to the credit reference sector stipulate that consent of a *data subject* must be in writing. The Personal Data Protection Regulations relating to the banking sector provide that the consent of a *data subject* must be obtained in writing if a financial institution provides the personal data of that *data subject* to a third party.

There are no explicit formalities for obtaining consent in the Personal Data Protection Guidances. However, it is advisable to obtain consent in writing and preferably in hard copy.

Sensitive Personal Data

What is sensitive personal data?

The Personal Data Protection Regulations generally do not explicitly distinguish between personal data and the *standard types of sensitive personal data*.

The Personal Data Protection Guidelines define sensitive personal data as information, the disclosure or modification of which may have a negative effect on the *data subject*. Sensitive personal data may include ID numbers, cell phone numbers, racial or ethnic origin, political opinions, religious beliefs, genes and figureprints. This is broader than the *standard types of sensitive personal data*.

The Personal Data Protection Guidelines state that the express consent of the *data subject* should be obtained when processing sensitive personal data. In addition, organisations should refrain from directly collecting sensitive personal data from persons with limited or without capacity for civil conduct. When collecting sensitive personal data of such a person, the express consent of the legal guardian of such person should be obtained.

Are there additional rules for processing sensitive personal data?

Generally, there are no additional rules in the Personal Data Protection Regulations. However, the regulations relating to the credit reference sector prohibit credit reference agencies from collecting certain information, such as information about religious beliefs, genes, figureprints, blood types or medical histories of any individuals.

The Personal Data Protection Guidelines state that when the purpose of processing sensitive personal data has been achieved, the express consent of the *data subject* is required to be obtained if such sensitive personal data will be further processed.

Are there any formalities to obtain consent to process sensitive personal data?

There are no uniform formalities in the Personal Data Protection Regulations. However, the Personal Data Protection Regulations relating to the credit reference sector stipulate that consent of a *data subject* must be in writing. The Personal Data Protection Regulations relating to the banking sector provide that the consent of a *data subject* must be obtained in writing if a financial institution provides the personal data of that *data subject* to a third party.

There are no explicit formalities for obtaining consent in the Personal Data Protection Guidances. However, it is advisable to obtain consent in writing and preferably in hard copy.

People's Republic of China.

Scope of Application

What is the territorial scope of application?

The territorial application of each individual Personal Data Protection Regulation that is applicable to a particular instance of collection and use of data varies. The Personal Data Protection Regulations generally do not contain express provisions on their territorial effect. However, Personal Data Protection Regulations promulgated by a provincial authority would generally only apply to entities which collect and use personal data in that province.

Who is subject to data protection legislation?

Any individual or institution collecting and using personal data in a province or sector to which a Personal Data Protection Regulation applies is required to comply with that Personal Data Protection Regulation. The Personal Data Protection Regulations do not generally distinguish between *data controllers* and *data processors*.

The Personal Data Protection Guidelines distinguish between "administrators of personal data" and "receivers of personal data". The former refers to the organization or institution which determines the purpose and means of the processing of personal data and which controls and processes the personal data. The latter refers to the individual, organization or institution which receives the personal data from an information system and processes such information in accordance with the will of the *data subject*. The concept of the "administrator of personal data" is similar to *data controller*.

Are both manual and electronic records subject to data protection legislation?

Both manual and electronic records are subject to the Personal Data Protection Regulations.

The Personal Data Protection Guidelines only apply to the processing of the personal data through information systems.

Rights of Data Subjects

Compensation

Data subjects have a right to claim compensation for damages if a data collector infringes their civil rights, which under the laws of China includes a right of privacy. However, in practice, we are only aware of rare cases in which a *data subject* has received any such compensation.

Fair processing information

There are no uniform rules about providing *fair processing information* to *data subjects* in the Personal Data Protection Regulations. However, in the banking sector, informed consent must be obtained from a *data subject* before his or her personal data is provided to a *data processor*. Internet service providers, when collecting personal data, must clearly state the purpose, means and scope of their data collection to *data subjects* at the time of collection and cannot collect unnessary personal data or use the personal data for a purpose other than the stated purpose. In the telecoms sector, internet service providers must also obtain the consent of *data subjects* prior to disclosing personal data to others.

The Personal Data Protection Guidelines provide more detailed guidance on fair processing.

Rights to access information

There are no uniform rules about access to personal data in the Personal Data Protection Regulations. However, in the credit reference sector, a *data subject* is entitled to ask a credit reference agency to provide his or her own personal data, and has a right to acquire his or her own credit report from the credit reference agency for free twice a year.

Under the Personal Data Protection Guidelines, a *data subject* should be able to access their personal data. Generally, the administrator of personal data must inform the *data subject* regarding whether it owns his or her personal data, the contents of the personal data and the status of its processing.

Objection to direct marketing

There are no uniform rules about direct marketing. However, under the Personal Data Protection Regulations applying to the Internet sector, personal data may only be used for the purposes of direct marketing of goods or services with the consent of the *data subject*. Under the Personal Data Protection Regulations relating to the banking sector, a banking financial institution may not use personal data for marketing purposes other than for those marketing purposes for which the data was collected.

Other rights

Under certain of the Personal Data Protection Regulations relating to Internet service providers, a *data subject* may request the person or institution in charge of the processing to rectify, block or delete personal data.

The Personal Data Protection Guidelines grant similar rights to *data subjects*.

Security

Security requirements in order to protect personal data

The Personal Data Protection Regulations do not impose uniform or detailed security requirements. However, some sector-specific regulations (particularly in the credit reference, banking and Internet sectors) impose general obligations to maintain personal data securely.

The Personal Data Protection Guidelines state that organisations should have in place necessary and sufficient administrative and technical measures to ensure the safety of personal data.

Specific rules governing processing by third party agents (processors)

There are no uniform rules about processing of personal data by *data processors*. However, the Personal Data Protection Regulations relating to the banking sector require banks and financial institutions to properly evaluate their outsourced service providers and ensure that such providers adequately protect personal data that may be disclosed to them.

Notice of breach laws

There are no uniform rules requiring entities to notify any particular agency or person if there has been a breach of privacy. However, in the banking sector, where divulgence of any personal financial data occurs in breach of the banking regulations, the banking financial institution must promptly inform the People's Bank of China. Internet service providers must notify the MIIT of any divulgence of personal data where serious consequences are or may be caused by that divulgence.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

There are no uniform rules about cross-border transfers of personal data in the Personal Data Protection Regulations. However, the Personal Data Protection Regulations that relate to the banking sector stipulate that personal financial information collected within China must be processed inside China. Offshore entities may not be provided with such information unless explicitly permitted by another law or regulation. The Personal Data Protection Regulations relating to the credit reference sector impose similar restrictions.

Under the Personal Data Protection Guidelines, the administrator of personal data can transfer personal data to individuals, organisations or insitiutions outside of China only if: (i) it obtains the express consent from the *data subject* or competent authority; or (ii) any law or regulation allows it to do so.

Notification and approval of national regulator (including notification of use of Model Contracts)

There are no uniform rules requiring that cross-border transfers of personal data are notified to or approved by any regulator.

Use of binding corporate rules

There are no rules relating to the use of *binding corporate rules*.

Enforcement

Sanctions

Sanctions for contravention of the Personal Data Protection Regulations will depend on the Personal Data Protection Regulation that has been contravened and the nature of that contravention. Sanctions may include administrative sanctions, such as a warning, fines (generally up to RMB 30,000, although certain regulations apply higher penalties), confiscation of profit arising from the violation and suspension or revocation of operating licences. Affected parties may be able to seek civil compensation in certain cases.

Under the Chinese Criminal Law, staff of certain organisations (including State-owned organisations and financial, telecommunications, transport, education and medical organisations) may be imprisoned for up to three years for selling or illegally providing to others personal data obtained in the course of their employment.

Practice

The number of administrative and criminal cases relating to the violation of the Personal Data Protection Regulations has increased in recent years. There have been some cases of individuals being imprisoned for selling personal data in violation of the Chinese Criminal Law provision outlined above.

Enforcement authority

There is no single enforcement authority. The Personal Data Protection Regulations are enforced by the courts, the public security department, the industrial and commercial administrative department and various other regulatory authorities, especially those with supervisory powers over the credit reference, banking, telecommunications and Internet sectors.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The principal regulation on ePrivacy is the *Resolution of the Standing Committee of the National People's Congress relating to Strengthening the Protection of Information* on the Internet which was issued at the end of 2012. This is the first general law relating to ePrivacy. Some of the other Personal Data Protection Regulations issued by China's other competent regulatory authorities (such as the MIIT) also include provisions that relate to electronic privacy, for example, the *Measures for the Administration of Internet E-mail Services* (promulgated in early 2006) include rules relating to marketing by e-mail (collectively, the "**Electronic Privacy Regulations**").

Cookies

Conditions for use of cookies

There are no specific requirements or conditions relating to the use of cookies under the Electronic Privacy Regulations.

Regulatory guidance on the use of cookies

None.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The Electronic Privacy Regulations stipulate that no individual or institution may send commercial electronic information by e-mail: (i) prior to obtaining the consent of the receiver or upon the receiver's request; (ii) if the receiver explicitly refuses to receive such information; or (iii) unless the sender includes in the subject heading of the e-mail the words "advertisement" or "AD" (or the equivalent in Chinese as prescribed by the regulations). Furthermore, when sending commercial advertisements by e-mail, a sender must provide recipients with its contact information to allow recipients the ability to 'opt out' or 'unsubscribe'. The Electronic Privacy Regulations do not provide for any formalities that senders must follow when soliciting consent.

Other Personal Data Protection Regulations include provisions relating to direct marketing irrespective of the means of communication used. For example, under the Personal Data Protection Regulations relating to the banking sector, a banking financial institution may not use personal data for marketing purposes other than for those marketing purposes for which the data was collected.

Conditions for direct marketing by e-mail to corporate subscribers

The Electronic Privacy Regulations, in respect of direct marketing, only apply to individuals and not corporate subscribers.

Exemptions and other issues

It is illegal to send advertising text messages to mobile phones prior to obtaining a licence from the MIIT. Otherwise the Electronic Privacy Regulations do not include any more detailed rules except for the general requirements set out above.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

The Electronic Privacy Regulations stipulate that no individual or institution may send commercial electronic information through fixed line telephones or mobile phones: (i) prior to obtaining the consent of the receiver or upon the receiver's request; or (ii) if the receiver explicitly refuses to receive such information. However, the Electronic Privacy Regulations do not provide for any formalities that senders must follow when soliciting consent or for receivers to 'opt out' or 'unsubscribe'. In addition, it is illegal to send advertising text messages to mobile phones prior to obtaining a licence from the MIIT.

Other Personal Data Protection Regulations include provisions relating to direct marketing irrespective of the means of communication used. For example, under the Personal Data Protection Regulations relating to the banking sector, a banking financial institution may not use personal data for marketing purposes other than for those marketing purposes for which the data was collected.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The Electronic Privacy Regulations, in respect of direct marketing, only apply to individuals and not corporate subscribers.

Exemptions and other issues

The Electronic Privacy Regulations do not include any more detailed rules except for the general requirements set out above.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

There are no uniform rules in the Electronic Privacy Regulations for marketing by fax.

Certain other Personal Data Protection Regulations include provisions relating to direct marketing irrespective of the means of communication used. For example, under the Personal Data Protection Regulations relating to the banking sector, a banking financial institution may not use personal data for marketing purposes other than for those marketing purposes for which the data was collected.

Conditions for direct marketing by fax to corporate subscribers

The Electronic Privacy Regulations, in respect of direct marketing, only apply to individuals and not corporate subscribers.

Exemptions and other issues

The Electronic Privacy Regulations do not include any more detailed rules except for the general requirements set out above.

The contents set out above do not constitute any opinion or determination on, or certification in respect of, the application of PRC law. Any comments concerning the PRC are based on our transactional experience and our understanding of the practice in the PRC. Like all international law firms with offices in the PRC, Linklaters LLP and its affiliated firms and entities (including Linklaters in Hong Kong) are not licensed to undertake PRC legal services. We have standing arrangements with a number of PRC lawyers. If you would like advice on the application of PRC law or other PRC legal services, please let us know and we would be pleased to make any necessary arrangements on your behalf.

Poland.

General | Data Protection Laws

National Legislation

General data protection laws

The Act on the Protection of Personal Data of 29 August 1997 (Journal of Laws of 2002, No. 101, Item 926, as amended) (the "**DPA**") implemented the *Data Protection Directive* in Poland.

Entry into force

The DPA entered into force on 30 April 1998.

National Regulatory Authority

Details of the competent national regulatory authority

The Inspector General for the Protection of Personal Data (the "**IGPPD**")
ul. Stawki 2
00-193 Warsaw
Poland

www.giodo.gov.pl

Notification or registration scheme and timing

A *data controller* must give notification of any data filing system with the IGPPD before starting to process the data in a data filing system. In the event of data filing systems containing sensitive data, the *data controller* may only start to process these data after its registration. The IGPPD may refuse registration.

From 1 January 2007, notification of any data filing system and registering changes are free of charge.

Exemptions

The obligation to register filing systems does not apply to certain *data controllers*. Such exemptions apply when: (i) the data include classified information; (ii) the data were obtained as a result of operational and official investigative acts of authorities entitled to perform such acts; (iii) the data were processed by the relevant authorities for the purposes of court proceedings and pursuant to the National Criminal Register; (iv) the data were processed by the General Inspector of Financial Information or for purposes of the Schengen Information System or Visa Information System; (v) the data concern members of a church or other religious society; (vi) the data are processed in connection with employment by the *data controllers* or providing services to the *data controllers* under civil law agreements; (vii) the data are processed in connection with providing medical, notarial, legal, patent agent, auditor and tax advice services; (viii) the data are created on the basis of electoral regulations; (ix) the data refer to persons deprived of freedom under the relevant law; (x) the data are processed exclusively in connection with issuance of an invoice, receipt or financial reporting; (xi) the data are commonly accessible; (xii) the data are processed to allow graduation from higher education; or (xiii) the data are processed in relation to minor, current matters of everyday life.

Appointment of a data protection officer

The *data controller* must appoint a data security controller to ensure fulfilment of the data security rules, unless the *data controller* performs such duty by itself. Therefore, if a *data controller* is a natural person, then such person may also supervise fulfilment of the data security rules. In the case of the *data controller* being a legal person, a data security controller should be appointed. The data security controller can be either an employee of the *data controller* or an independent person acting on the basis of a relevant agreement.

Personal Data

What is personal data?

The definition in the DPA is based on the *standard definition of personal data*. In particular, information is not personal data if identifying the relevant individual would require an unreasonable amount of time, cost and manpower.

Is information about legal entities personal data?

No. Information relating to sole traders and partnerships or other legal entities registered in the commercial activity register is not personal data.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met, with the exception of processing to protect a vital interest of a *data subject* if a *data subject's* consent cannot be obtained.

Are there any formalities to obtain consent to process personal data?

The consent of a *data subject* does not need to be in writing (unless it regards sensitive data) but cannot be presumed, must be expressed clearly and specifically, and must be given freely. The consent may also cover the processing of data in the future, provided the purpose of processing is unchanged.

However, obtaining consent from employees may be difficult as, in some cases, it may be hard to demonstrate that consent has been given freely by the employee. In addition, the Supreme Administrative Court has confirmed that an employer can only obtain effective consent from its employees for the processing of their personal data in the situations specifically set out in Polish labour law.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data include both: (i) the *standard types of sensitive personal data*; and (ii) personal data revealing religious or party adherence, data concerning genetic code, addictions and data relating to convictions, decisions on penalties or fines and other decisions issued in court or administrative proceedings.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met.

Additionally conditions apply allowing the processing of sensitive personal data if a specific legal act permits their processing, the processing is for scientific research or for the purposes of execution of rights or obligations arising out of rulings issued in court or administrative proceedings.

Are there any formalities to obtain consent to process sensitive personal data?

Consent to the processing of sensitive personal data must be given in writing.

Scope of Application

What is the territorial scope of application?

The DPA uses the *standard territorial test*.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA.

Are both manual and electronic records subject to data protection legislation?

The DPA applies to the processing of personal data in: (i) files, indexes, books, lists and other registers; and (ii) computer systems, including where data are processed outside of a data filing system.

Where personal data files are prepared: (i) ad hoc; (ii) exclusively for technical, training, or higher education purposes; and (iii) to be immediately removed or rendered anonymous after use, they are only subject to the provisions regarding protection and security measures.

Rights of Data Subjects

Compensation

The DPA does not contain specific provisions regarding compensation for *data subjects*. However, *data subjects* should be able to obtain compensation for breach of the DPA under the general rules of the Polish Civil Code.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. In addition a *data controller* must inform *data subjects* of the recipients or categories of recipients, the right to access and correct their personal data and whether the providing of personal data to a *data controller* is voluntary or mandatory. When the provision of personal data is mandatory, the legal grounds for such obligation should also be indicated. Where the data are not collected from *data subjects*, information on the scope and source of the data, as well as the right to object, shall be provided.

There is no obligation in the DPA to provide this information in Polish, though it may be difficult to show the information has been fairly provided if it is not in a language the *data subject* is familiar with.

Rights to access information

Data subjects may obtain their *subject access information* by request to *data controllers.* This right may only be exercised once every six months and the *data controller* must respond within 30 days of the request.

Objection to direct marketing

In certain circumstances a *data subject* may require that a *data controller* stops processing his personal data for direct marketing purposes or that a *data controller* stops transferring the data to other *data controllers*. In the case of such requirement, further processing of data by the *data controller* is prohibited.

Other rights

Data subjects have a right to control the processing of their personal data contained in the filing systems, and in particular have the right to correct their data and to object to their data being processed.

Data subjects have the right to demand that the data be completed, updated, rectified, temporarily or permanently suspended or erased, if they are incomplete, outdated, untrue or collected in violation of the DPA, or if they are no longer required for the purpose for which they were collected.

Data subjects also have the right to file a substantiated demand in writing, in certain cases, to have the data processing halted. If the *data controller* refuses the demand, it is submitted to the IGPPD for decision.

Data subjects can also demand that the *data controller* review a resolved matter again on the basis of an automated decision.

Security

Security requirements in order to protect personal data

Data controllers must comply with the *general data security obligations*. Regulations were issued in 2004 setting out basic, medium and high levels of security, including details of the specific measures that must be employed by the *data controller*.

Specific rules governing processing by third party agents (processors)

A *data controller* may authorise another entity to carry out the processing of the personal data by way of a written contract if it obliges the *data processor* to comply with the *standard processor obligations*. The *data processor* may process the data solely in the scope and for the purpose laid down in the contract and must take the data security measures described in the DPA before proceeding to process the data. The *data controller* remains responsible under the DPA for the proper processing of the data. However, the *data processor* may be liable under contract.

Notice of breach laws

The DPA does not contain any obligation to inform the IGPPD or the *data subject* of a security breach.

Specific notice of breach laws will apply to the electronic communications sector once the amendments to the TL (as defined below) enter into force on 22 March 2013. The amendment obliges providers of public telecommunication services to inform the IGPPD of a personal data security breach within three days of such breach. In certain situations *data subjects* should also be informed of breaches of their personal data.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Personal data may be transferred if the *standard conditions for transborder dataflow* are met, provided that any transfer based on the *Model Contracts* or *binding corporate rules* is only allowed upon obtaining prior consent of the IGPPD. Please note that the *data subject's* consent must be expressed in writing. Please note that according to the express wording of Article 47 of the DPA, transborder dataflow is permitted if transferred data are publicly available. Such wording is different from the wording of Article 26 of the Directive, as it is not limited to dataflow from a public register but instead refers to a general category of data publicly available, without distinguishing where the dataflow is from.

Notification and approval of national regulator (including notification of use of Model Contracts)

In situations other than those detailed above, the transfer may take place subject to the prior approval of the IGPPD, provided that the *data controller* has installed safeguards to the extent of the protection of the privacy and rights and freedoms of *data subjects*. Although notification of use of *Model Contracts* may be helpful when applying to the IGPPD for gaining transfer approval, the IGPPD issues its approval at its exclusive discretion.

Use of binding corporate rules

The IGPPD does not recognise the use of *binding corporate rules* as a separate ground legitimising transfers of personal data outside the EEA. However, notification of *binding corporate rules* may be helpful when applying for the IGPPD's approval to any *transborder dataflows*, e.g. the approvals for *transborder dataflows* issued to Hyatt and J.P. Morgan were based on their *binding corporate rules*.

Enforcement

Sanctions

A breach of the DPA would give rise to criminal liability, including a fine (varying between PLN 100 and PLN 1,080,000), a partial restriction of freedom or a prison sentence of up to three years.

Practice

According to the IGPPD, there were 139 inspections conducted by it in 2012. The IGPPD received 1,306 complaints regarding infringement of the DPA and it has filed 10 notices about criminal offences to the proper prosecuting bodies.

There were 1,009 decisions issued; 319 from the Registration Department, 51 from the Inspection Department and 629 from the Legislation and Claims Department.

Enforcement authority

The IGPPD may issue an administrative decision demanding the situation be returned to a state compliant with law, in particular that: (i) the negligence be remedied; (ii) the personal data be completed, updated, corrected, disclosed or not disclosed; (iii) additional measures be applied in protecting the personal data; (iv) the flow of personal data to a third country be suspended; (v) the data be safeguarded or transferred to other entities; or (vi) the personal data be erased.

The IGPPD can inform proper prosecuting bodies about infringement of the DPA in order for them to instigate criminal proceedings. Although the IGPPD has no direct power to impose financial penalties, since March 2011 it is authorised to fine those who failed to comply with its decision. Fines for natural persons vary from up to PLN 10,000, for one fine in one proceeding, to PLN 50,000 if several fines are imposed in one proceeding. Fines for legal entities vary up to PLN 50,000 if one fine is imposed to PLN 200,000 where several fines are imposed in one proceeding.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Act on the Provision of Services by way of Electronic Means, dated 18 July 2002 (Journal of Laws of 2002, No. 144, Item 1204) (the "**ECA**"), which entered into force on 10 March 2003, and the Telecommunication Law dated 16 July 2004 (Journal of Laws of 2004, No. 171, Item 1800) (the "**TL**"), the majority of which entered into force on 3 September 2004, together implemented Article 13 of the *Privacy and Electronic Communications Directive*.

The ECA and TL have recently been amended to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

According to the amendment of the TL regarding cookies, entering into force on 22 March 2013, it is necessary to provide users with information relating to: (i) the purpose of storing and obtaining access to information; and (ii) the ability of the user to determine the conditions of storage or access using software settings or by configuring the service. Once the information is provided and the user grants consent, the cookies can used. A user may express their consent by accepting the configuration of the service or the default settings of the browser they is using.

Regulatory guidance on the use of cookies

There is currently no guidance on the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing by e-mail is authorised if the recipient gave his prior consent to receiving such e-mails, in particular by disclosing his e-mail address for that purpose. The consent cannot be presumed and can be revoked at any time.

Conditions for direct marketing by e-mail to corporate subscribers

Provisions on direct marketing by e-mail are not applicable to corporate subscribers.

Exemptions and other issues

The ECA imposes a range of conditions on any direct marketing, including a requirement that the entity sending the marketing material identify itself and provide an e-mail address.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing by telephone is permitted if certain conditions are fulfilled, including restrictions imposed by the Law on Counteracting Unfair Market Practices, dated 23 August 2007 (Journal of Laws 2007 No. 171 Item 1206) (the "**CUMP**"), and particularly those in relation to aggressive marketing practices. However, according to the Law on Protection of Certain Consumers' Rights and Liability for Dangerous Product, dated 2 March 2000 (Journal of Laws 2000 No. 22 Item 271, as amended) (the "**CCR**"), the use of the telephone for the purpose of making an offer to conclude an agreement is permitted solely upon the individual's prior consent.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The rules on direct marketing by telephone are not applicable in relation to corporate subscribers.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax is authorised if certain conditions are fulfilled, including restrictions imposed by the CUMP. However, according to the CCR, the use of fax for the purpose of making an offer to conclude an agreement is permitted solely upon the individual's prior consent.

Conditions for direct marketing by fax to corporate subscribers

The rules on direct marketing by fax are not applicable in relation to corporate subscribers.

Exemptions and other issues

No exemptions apply.

Portugal.

General | Data Protection Laws

National Legislation

General data protection laws

Directive 95/46 has been implemented by Law 67/98 of 26 October on personal data protection (the "**DPA**").

Entry into force

The DPA came into force on 1 November 1998.

National Regulatory Authority

Details of the competent national regulatory authority

Comissão Nacional de Protecção de Dados (the "**CNPD**")
Rua de São Bento, n.° 148, 3°
1200-821 Lisboa
Portugal

www.cnpd.pt

Notification or registration scheme and timing

The *data controller* must notify the CNPD before carrying out any wholly or partly automatic processing of personal data.

In addition, the prior authorisation of the CNPD is required for: (i) the processing of sensitive personal data if that processing does not satisfy a limited range of processing conditions (see "Are there additional rules for processing sensitive personal data?" below). Authorisation will only be given if such processing is essential for the exercise of the legal or statutory rights of the *data controller* or when the *data subject* has given his explicit consent for such processing; (ii) the processing of data relating to illegal activities or offences. This type of personal data may only be created and kept by public authorities vested with that specific responsibility; (iii) the processing of data relating to the credit and solvency of the *data subjects*; (iv) the use of personal data for purposes other than those which determined their collection; and (v) the combination of personal data not provided for in a legal provision. The non-automatic processing of sensitive personal data shall also be subject to authorisation.

Notification costs EUR 75 and authorisation costs EUR 150. If an authorisation request is particularly complex, the CNPD may increase the fee to half the monthly minimum wage in Portugal (currently EUR 485).

Exemptions

The CNPD may simplify, or create exemptions to, notification for particular categories of processing that are unlikely, taking account of the data to be processed, to adversely affect the rights and freedoms of the *data subjects*.

So far the CNPD has issued six exemptions from notification for: (i) processing of employees' salaries and benefits; (ii) management of libraries' and archives' users; (iii) invoicing and contacts with clients, suppliers and service providers; (iv) administrative management of employees, staff and service providers; (v) access control (entries and exits) in buildings; and (vi) collection of quotas for membership in associations and contacts with affiliates.

Processing of personal data necessary in order to keep a public register is also exempted from notification.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The definition of personal data in the DPA is similar to the *standard definition of personal data*.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the legitimate interests condition is frequently relied upon as grounds for processing non-sensitive personal data.

The DPA contains exemptions for certain types of processing. For example, processing of personal data carried out by a natural person in the course of a purely personal or household activity is exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

Consent must be freely given, specific, informed and unambiguous. There is no obligation for consent to be in writing. However, the CNPD expects *data controllers* to maintain a record of consents given by *data subjects* so in practice consent is normally obtained in writing.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data means data on philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and concerning health or sex life, including genetic data. Therefore, the concept of sensitive personal data under the DPA is largely similar to the *standard types of sensitive personal data* but also includes genetic data and data on the private life of the *data subject*.

Information about illegal activities and offences is also subject to additional restrictions.

Are there additional rules for processing sensitive personal data?

The processing of sensitive personal data is permitted if it: (i) is necessary to protect the vital interests of the *data subject* or of another person; (ii) is carried out with the *data subject's* consent by a non-profit seeking body; (iii) relates to data made public by the *data subject*; (iv) is necessary for the establishment, exercise or defence of legal claims; (v) relates to health and sex life, including genetic data; and (vi) is necessary for medical reasons.

The authorisation of the CNPD is needed in any other case (including where processing is based on the consent of the *data subject*). Authorisation will only be awarded: (i) when such processing is essential for exercising the legal or statutory rights of the *data controller*; or (ii) when the *data subject* has given his/her explicit consent for such processing.

The processing of personal data relating to illegal activities or offences is also subject to prior authorisation. Furthermore, central registers relating to persons suspected of illegal activities or found guilty of offences, may only be created and kept by public authorities vested with that specific responsibility.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be freely given, specific, informed and explicit. There is no obligation for consent to be in writing. However, the CNPD expects *data controllers* to maintain a record of consents given by *data subjects* so in practice consent is normally obtained in writing.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The person responsible for compliance with the DPA is the *data controller*. Where the purposes and means of processing are determined by laws or regulations, the *data controller* shall be designated in the statute establishing the organisation and functioning, or in the articles of association of the legal or statutory body competent to protect the personal data concerned.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies personal data processed wholly or partly by automatic means or on a manual filing system.

Rights of Data Subjects

Compensation

Any person who has suffered damages as a result of an unlawful processing operation or any other breach of personal data legislation is entitled to receive compensation from the *data controller* for the damage suffered. The *data controller* may be exempted from this liability, in whole or in part, if it proves that it was not responsible for the event giving rise to the damage.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. The *data controller* must also provide other information such as the recipients or categories of recipients, whether replies are mandatory or voluntary, and the existence and conditions of the right of access and the right to rectify, provided they are necessary, taking into account

the specific circumstances of collection of the data, in order to guarantee to the *data subject* that they will be processed fairly.

Rights to access information

The *data subject* has the right to obtain his/her *subject access information* by written request to *data controllers* at reasonable intervals and without excessive delay or expenses.

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing his/her personal data for direct marketing purposes or any other form of research. The *data controller* must then cease such processing within a reasonable period.

Other rights

The *data subject* has the right to obtain from the *data controller* the rectification, erasure or blocking of data, the processing of which does not comply with the DPA and the right of notification to third parties to whom the data has been disclosed of any such rectification, erasure or blocking.

The *data subject* has the right to object at any time, on compelling legitimate grounds relating to his/her particular situation, to the processing of data relating to him/her.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations*. These include measures to: (i) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes; (ii) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and (iii) ensure the implementation of a security policy with respect to the processing of personal data.

The National Communications Authority, ICP-ANACOM, is able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

A *data controller* who processes sensitive personal data under an authorisation of the CNPD or who processes personal data relating to illegal activities or offences must take additional measures.

These additional measures require the *data controller* to: (i) prevent unauthorised access to the premises used for processing such data; (ii) prevent data media from being read, copied, altered or removed by unauthorised persons; (iii) prevent unauthorised input and/or control over inputs; (iv) prevent unauthorised use of processing equipment; (v) prevent unauthorised access to data; (vi) confirm the details of the persons to whom the data is transmitted; (vii) keep an audit trail of all inputs; and (viii) protect information while it is being transmitted (which at the CNPD's direction may include encryption). Furthermore, the systems used must guarantee the logical separation between data relating to health and sex life, including genetic data, and other personal data.

Specific rules governing processing by third party agents (processors)

The *data processor* chosen by the *data controller* must provide sufficient guarantees with respect to the technical security measures and organisational measures governing the processing to be carried out and must ensure compliance with those measures.

There must be a contract or legal act binding the *data processor* to the *data controller* and stipulating in particular that the *data processor* shall comply with the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any obligation to inform the CNPD or the *data subjects* of a security breach.

Law 46/2012, which implemented the *Citizens' Rights Directive*, requires providers of electronic communications to promptly inform the CNPD whenever there is a breach of personal data.

Electronic communication providers must also promptly inform *data subjects* whose data has been breached of that fact, if the breach negatively affects the *data subject* and appropriate technological protection measures have not been used to render the affected data unreadable.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transfer of personal data to a country that is not a member of the EU may only take place provided that that country ensures an adequate level of protection or the *standard conditions for transborder dataflow* are satisfied. It is for the

CNPD to decide whether a State which is not a member of the European Union ensures an adequate level of protection. However, in 2004 the CNPD issued an interpretative notice stating that it would follow any decision by the European Commission considering that an adequate level of protection exists.

Notification and approval of national regulator (including notification of use of Model Contracts)

All transfers of data must be notified to the CNPD.

Furthermore, all transfers of data to countries outside the EEA are subject to prior authorisation from the CNPD unless they are to whitelisted countries or made under the *Model Contracts*.

Use of binding corporate rules

The CNPD has not approved the use of *binding corporate rules*.

Enforcement

Sanctions

The sanctions have a quasi-criminal and criminal nature: the imposition of fines of up to EUR 30,000 and imprisonment for up to four years. In addition, the entity that breaches the DPA is liable, under general legal rules of law, for the damages caused to the *data subject* or third parties.

Practice

The number of investigations and prosecutions is not publicly available.

There have been no significant fines publicised recently. The highest fine imposed so far is the EUR 20,000 fine applied to Radiotelevisão Portuguesa, S.A. ("**RTP**"), the public television company, in April 2004. This fine was imposed as a result of RTP reviewing the professional skills of its employees. It hired a company to assess various pieces of data about its workers but failed to notify its employees of this assessment process. Under Portuguese law, RTP was obliged to notify the CNPD before carrying out such a data processing operation. RTP also informed the contractor about the trade union membership of its employees, which was not authorised by CNPD or consented to by the *data subjects*. The CNPD also found that RTP had a video surveillance system in operation in its building which had not been authorised by the CNPD.

In general, the level of fines are lower than this and are mainly applied for unauthorised disclosure of health information, keeping credit history details for an excessive period or video surveillance.

Enforcement authority

The CNPD has the power to investigate *data controllers*, including by carrying out dawn raids. Following an investigation it can apply fines. *Data controllers* can appeal to the courts against those fines.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Article 13 of the *Privacy and Electronic Communications Directive* has been implemented by Decree-Law No. 7/2004 of 7 January 2004 (the "**ECA**"). Currently, the provisions regarding unsolicited communications and direct marketing are laid down by Law 41/2004, as amended by Law 46/2012 ("**Law 41/2004**").

Cookies

Conditions for use of cookies

According to Law 46/2012, which implemented the *Citizens' Rights Directive* into Portuguese law, the use of cookies is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with the DPA, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access if it is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service, explicitly requested by the subscriber or user, to provide the service.

Regulatory guidance on the use of cookies

None.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing by e-mail to individual subscribers is authorised provided the addressee gives its prior consent.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing by e-mail to corporate subscribers is permitted without their prior consent but they must be given the right to object to this marketing at any time.

Exemptions and other issues

It is permitted to send e-mail for the purposes of direct marketing if the *similar products and services exemption* applies. Law 41/2004 also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; (ii) an opt-out address is not provided; or (iii) the e-mail encourages recipients to visit websites that do not clearly identify: (a) the promotional nature of the message; (b) the advertiser; and (c) promotional offers, such as discounts, premiums and gift promotional competitions or games, and their respective terms and conditions.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing by telephone to individual subscribers is permitted without their prior consent but they must be given the right to object to this marketing at any time.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Direct marketing by telephone to corporate subscribers is permitted without their prior consent but they must be given the right to object to this marketing at any time.

Exemptions and other issues

None.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax to individual subscribers is authorised provided the addressee gives its prior consent.

Conditions for direct marketing by fax to corporate subscribers

Direct marketing by telephone to corporate subscribers is permitted without their prior consent but they must be given the right to object to this marketing at any time.

Exemptions and other issues

None.

Romania.

Contributed by Kinstellar

General | Data Protection Laws

National Legislation

General data protection laws

Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and Free Circulation of Such Data, published in the Official Gazette No. 790 of 12 December 2001 (the "**DPA**") implemented the *Data Protection Directive*.

Entry into force

The provisions of the DPA came into force on 12 December 2001.

National Regulatory Authority

Details of the competent national regulatory authority

The National Supervisory Authority for Personal Data Processing (the "**Supervisory Authority**").

28-30 Magheru Blvd.
Bucharest, Sector 1
Romania

www.dataprotection.ro

Notification or registration scheme and timing

Personal data may not be processed by a *data controller* that has not submitted a notification, personally or through a representative, to the Supervisory Authority, unless an exemption applies. The notification must be submitted prior to any processing of personal data and at least 30 days prior to processing of sensitive data. There is no fee for filing the notification. The notification can also be made online.

Exemptions

The DPA and the Supervisory Authority's Decisions No. 90/2006, No. 100/2007 and No. 23/2012 set out a wide range of situations in which the notification of personal data processing is not required, such as processing: (i) for public records; (ii) by public authorities; (iii) limited to certain employee data and external co-workers; (iv) for property management matters; (v) for the management of share schemes; (vi) for recruitment purposes; (vii) of contact data for business purposes; (viii) by non-commercial entities; (ix) by cults or religious organisations; (x) in relation to the National Council for the Study of the Security Archives; (xi) done exclusively for journalistic, literary or artistic purposes; (xii) regarding the participants to seminars, conferences and other similar events; (xiii) referring to the contact persons of public or private entities; (xiv) for performance of an authorised independent activity; (xv) for management of the National Archive database; (xvi) for the purposes of lending books, cinematography work, artistic work, other audio-visual works or copies thereof; (xvii) for the purpose of brokering real estate transactions; or (xviii) for processing personal data of members of political parties.

Additional derogations may be granted for non-profit making organisations, or by an express decision of the Supervisory Authority where the processing does not, or is unlikely to, infringe the rights of the *data subject*.

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer. Nonetheless, the appointment of a data protection officer may assist with data protection compliance and the handling of inspections by the Supervisory Authority.

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met or if: (i) it is necessary for statistical purposes, historical or scientific research; or (ii) the personal data are obtained from publicly available documents.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

The DPA requires that consent for processing be express and unequivocal. The DPA does not explicitly require that consent must be in writing. However, as a matter of practice, written consent is normally obtained as it provides significant evidential advantages.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data include: (i) the *standard types of sensitive personal data*; (ii) information about offences, criminal convictions, security measures and administrative sanctions; and (iii) a personal numeric code or other identifier having general application, such as an identity card, passport number, driving licence number, social or health security number.

Are there additional rules for processing sensitive personal data?

Processing of sensitive personal data is prohibited unless the *standard conditions for processing sensitive personal data* apply.

With respect to the processing of personal numeric codes, identity card details, passport number, driving licence number, or social or health security number, secondary legislation came into force providing for a higher degree of protection for these types of data (i.e. the consent of the *data subject* has to be expressed in a free, express, specific and informed manner, the *data controller* has to be able to provide evidence of such consent and the processing has to be adequate, relevant and non-excessive).

Personal data related to: (i) the commission of an offence by a *data subject*; (ii) proceedings for an offence; or (iii) the criminal or administrative sanctions that a *data subject* has suffered may be processed only under the supervision of public authorities.

Are there any formalities to obtain consent to process sensitive personal data?

The position is the same as for the processing of personal data (see above). However, express and unequivocal consent is not required where processing is carried out exclusively for journalistic, literary or artistic purposes and the personal data: (i) were made public by the *data subject*; or (ii) are closely related to the quality of the public character of the *data subject*.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test* and also applies to the processing of personal data carried out in the framework of activities performed by diplomatic missions or consular offices of Romania.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the DPA. If the purpose and the ways of processing the personal data are established through, or are based on, a legislative act, the *data controller* is the individual or legal person, in public or private law, designated as *data controller* by, or based on, that legislative act. *Data processors* may process personal data only in accordance with the *data controller's* specific instructions, except when their actions are based on a legal obligation.

Are both manual and electronic records subject to data protection legislation?

Yes.

Rights of Data Subjects

Compensation

The *data subject* has the right to request in a court of law the protection of any rights guaranteed by the DPA as well as a right to complain to the Supervisory Authority. Any person suffering a loss as a consequence of unlawful processing of personal data may claim damages from the competent courts of law. The claim for damages filed in front of the court of law is exempt from stamp tax.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects* unless the *data subject* already has the relevant information. The Romanian legislation also specifically requires the provision of additional information about: (i) the recipients or the categories of recipients; (ii) whether provision of the requested information is mandatory and the

consequences of the refusal to provide it; (iii) the *data subject's* rights and the conditions under which these rights can be exercised; and (iv) any further information requested by the Supervisory Authority to be provided for that particular type of processing.

The obligation to provide information does not apply if the data have not been obtained directly from the *data subject* and: (i) the data processing is performed exclusively for journalistic, literary or artistic purposes and its application might reveal the source of the information; (ii) the data processing is performed for statistical, historical or scientific research; (iii) the supply of such data proves to be impossible or would involve a disproportionate effort towards the legitimate interest that might be damaged; or (iv) the recording or the disclosure of the data is required by law.

Rights to access information

A *data subject* may obtain *subject access information* (or confirmation that the data concerning him are not being processed by the *data controller*) from a *data controller* upon written, dated and signed request. The first request per year is exempt from any taxes. The *data controller* must communicate the requested information within 15 days of receipt of the request.

Objection to direct marketing

The *data subject* has the right to object at any moment, freely and without any explanation, to the processing of data concerning him for direct marketing purposes. The *data controller* must then cease such processing within a reasonable period, and inform the *data subject* of the name of the third party to whom the *personal data* were disclosed, within 15 days of receiving the request.

Other rights

In certain cases, the *data subject* may ask the *data controller* to rectify, update, block, erase or destroy data whose processing does not comply with the provisions of the DPA, notably incomplete or inaccurate data. The *data subject* may ask the *data controller* to transform into anonymous data any data where the processing did not comply with the provisions of the DPA. Any *data subject* may object in writing to the processing of data regarding him, at any moment, based on justified and legitimate reasons linked to his particular situation. In certain cases, a *data subject* may require the withdrawal, annulment or re-evaluation of decisions being made about him which are solely based on automatic processing.

Security

Security requirements in order to protect personal data

Data controllers must comply with the *general data security obligations* but may set their own safety procedures and policies.

Specific rules governing processing by third party agents (processors)

Data processing performed by an appointed *data processor* can only be initiated following a written contract concluded between the *data controller* and *data processor* requiring the *data processor* to comply with the *data controller's* instructions and the *general data security obligations*.

When appointing a *data processor*, the *data controller* must: (i) assign a person who can give sufficient guarantees regarding compliance with the *general data security obligations*; and (ii) ensure that such assigned person complies with these measures.

Notice of breach laws

The DPA does not contain any obligation to inform the Supervisory Authority or *data subjects* of a security breach.

Specific notice of breach laws apply to the electronic communications sector as per the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*, as implemented into national law (i.e. the obligation to notify without delay to the Supervisory Authority any breach of data security and, in certain cases, to inform the *data subject* of such breach).

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Transfers outside the EEA must be authorised by the Supervisory Authority prior to the transfer. Such authorisation may be granted by the Supervisory Authority for a data transfer to a destination state that does not offer an equal level of protection as the DPA where the *data controller* offers sufficient safeguards with respect to the protection of the fundamental rights of individuals (e.g. transfers based on *Model Contracts*). The *data controller* cannot make their own assessment about how well personal data will be protected in a jurisdiction outside the EEA.

However, transfers within the EEA and other states outside the EEA for which the European Commission recognises an adequate level of protection are permitted without authorisation if: (i) Romanian law is not breached; and (ii) prior

notification to the Supervisory Authority is given. These conditions do not apply if the transfer takes place under a special law or under an international convention ratified by Romania.

Notification and approval of national regulator (including notification of use of Model Contracts)

As set out above, any transfer outside the EEA must be notified to the Supervisory Authority including those based on the *Model Contracts*.

Nonetheless, such a notification is not required: (i) in case of a transfer based on a specific law or an international convention ratified by Romania, particularly if the transfer is made for the purpose of preventing, investigating or sanctioning of a criminal offence; or (ii) if the processing of data is performed exclusively for journalistic, literary or artistic purposes, if the data were made public expressly by the *data subject* or are related to the *data subject's* public quality or to the public character of the facts he/she is involved in.

Use of binding corporate rules

The Supervisory Authority has not yet approved the use of *binding corporate rules* in Romania.

Enforcement

Sanctions

Breaches, unless they are deemed to be a criminal offence under criminal law, may incur civil liability, which includes a maximum fine of RON 50,000 (the approximate equivalent of EUR 11,000) for failure to fulfil the obligations regarding confidentiality and enforcement of security measures.

Under the PECR (as defined below), specific sanctions are provided for the offences mentioned therein (e.g. lack of notifications as described in Notice of breach laws above), ranging between RON 5,000 (the approximate equivalent of EUR 1,100) and RON 100,000 (the approximate equivalent of EUR 22,000). For companies having a turnover exceeding RON 5,000,000 (the approximate equivalent of EUR 1,100,000), a sanction of up to 2% of their annual turnover may be applied.

Practice

The Supervisory Authority replaced the Romanian Ombudsman as enforcement authority on 1 January 2006. The statistics for 2011 indicate that the Supervisory Authority received 11,223 notifications in 2011. As regards the number of approvals for data transfers to countries outside the EEA, the latest information available relates to 2010, when 86 such data transfers were approved by the Supervisory Authority.

In 2011, the Supervisory Authority received 404 complaints and 124 reclamations, resulting in 141 investigations. As regards sanctions applied by the Supervisory Authority, the latest statistics available relate to 2011, when sanctions were applied in 91 cases (of which 45% were warnings and 55% were fines) out of the total number of 214 investigations conducted by the Supervisory Authority in the same period.

During 2011, the Supervisory Authority also received 90 requests for guidance to assist with the interpretation of the provisions of the DPA for public authorities and private persons, as well as continuing its information campaigns around the country.

Enforcement authority

The Supervisory Authority is independent of any public authority or private entity and it receives notifications from personal *data processors* and complaints filed by people whose rights may have been infringed. The Supervisory Authority has the power to control personal *data processors* and to apply administrative sanctions.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Law no. 506/2004 of 17 November 2004 regarding the processing of personal data and the protection of privacy in the electronic communications sector (the "**PECR**"), published in the Official Gazette No. 1101 of 25 November 2004 implemented Article 13 of the *Privacy and Electronic Communications Directive*. The PECR came into force on 28 November 2004 and has been amended in 2012 in order to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Under the PECR, storing cookies or gaining access to such data is permitted subject to obtaining the prior consent of the *data subject* after having been informed of the processing activity and of its purpose in a complete, accessible and clear manner. In case of third party access to cookies, additional information obligations have to be observed prior to obtaining the consent, such as informing the *data subject* of: (i) the general purpose of the processing activities performed by third parties; and (ii) the possibility of using internet browser settings or other similar technologies to erase the stored personal data or to refuse third party access to the above information.

The setting made by the *data subject* in the internet browser or other similar technology to give consent to the *data controller* for using cookies is considered to observe the legal provisions. The *data controller* is exempted from the obligation to obtain prior consent for using cookies when the processing: (i) is done exclusively for the purpose of transmitting a communication through an electronic communication network; and (ii) is strictly necessary for providing an information society service expressly requested by the respective *data subject*.

Regulatory guidance on the use of cookies

There is no regulatory guidance for the use of cookies.

Marketing by E-mail

Conditions for sending direct marketing by e-mail to individual subscribers

It is not permitted to transmit unsolicited direct marketing e-mail unless the recipient has expressly given his prior consent. The precise mechanism by which consent is obtained is not set out in the PECR.

Conditions for sending direct marketing by e-mail to corporate subscribers

It is not permitted to transmit unsolicited direct marketing e-mail unless the recipient has expressly given his prior consent. The precise mechanism by which consent is obtained is not set out in the PECR.

Exemptions and other issues

It is permitted to send e-mail for the purposes of direct marketing where the *similar products and services exemption* applies. It is always forbidden to send e-mail for purposes of direct marketing where: (i) the identity of the sender is disguised or concealed; and (ii) there is no valid address to which the recipient may send a request that such communications cease.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

As there are no specific provisions regulating live marketing by telephone, it could be said that there are no restrictions regarding direct marketing by telephone, since the consent for such marketing can be obtained directly from the *data subject* at the time of the call and not necessarily through a prior procedure.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

As there are no specific provisions regulating live marketing by telephone, it could be said that there are no restrictions regarding direct marketing by telephone, since the consent for such marketing can be obtained directly from the *data subject* at the time of the call and not necessarily through a prior procedure.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send unsolicited direct marketing faxes to individual subscribers unless the recipient has expressly given his prior consent.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send unsolicited direct marketing faxes to corporate subscribers unless the recipient has expressly given his prior consent.

Exemptions and other issues

No exemptions apply.

Russia.

General | Data Protection Laws

National Legislation

General data protection laws

The Russian Federal Law "On Personal Data" (No. 152-FZ, dated 27 July 2006) (the "**OPD Law**") contains similar provisions to those in the *Data Protection Directive*.

Entry into force

The majority of the provisions of the OPD Law came into force on 26 January 2007. The OPD Law was amended significantly in July 2011.

National Regulatory Authority

Details of the competent national regulatory authority

The Federal Service for Surveillance in the Sphere of Communications, Information Technologies and Mass Communications ("**Roscomnadzor**")

Kitaygorodsky pr. 7, bld. 2
109074 Moscow

http://www.rsoc.ru/

Notification or registration scheme and timing

Russian law does not contain the concepts *data controller* and *data processor*. Instead, the OPD Law applies to "**data operators**" (see below).

Personal data may be processed by a data operator only with prior written notification to Roscomnadzor, unless the processing is exempt. No approval is required and notification is free of charge. The notification must occur prior to the first processing of personal data.

Exemptions

Every data operator who is processing personal data must notify Roscomnadzor unless they are subject to an exemption. Exemptions apply if: (i) the data are processed under employment law; (ii) the data were received by the data operator in connection with a contract with the *data subject*, provided that such personal data are not transferred to or circulated among third parties without the *data subject's* consent and are only used to perform the contract or to enter into other contracts with the *data subject*; (iii) the data relate to certain processing by a public association or religious organisation; (iv) the data were made publicly available by the *data subject*; (v) the data only consist of the surname, first name and patronymic of the *data subject*; (vi) the data are necessary for granting one-time access to the *data subject* into the territory where the data operator is located; (vii) the data are part of information systems of personal data which are classified as state-automated information systems as well as state information systems of personal data under relevant legislation and created for the protection of the state and for ensuring public order; (viii) the data are processed without using automated equipment, in compliance with federal laws or other regulations that lay down the requirements for the protection of personal data and *data subjects'* rights; or (ix) the data are processed in accordance with legal requirements relating to the safety of transportation systems.

Appointment of a data protection officer

There is a legal requirement for a data operator to appoint such an officer.

The officer is responsible for ensuring compliance with the OPD Law including: (i) implementing appropriate internal controls over the data operator and its employees; (ii) making employees of the data operator aware of personal data related laws and regulations, internal (local) acts on data protection and other data protection requirements; and (iii) dealing with applications and requests from *data subjects*.

Personal Data

What is personal data?

The OPD Law defines personal data as any information directly or indirectly related to an identified or identifiable individual (the subject of the personal data).

This definition is, therefore, largely based on the *standard definition of personal data*.

Is information about legal entities personal data?

No. However, information about sole traders or individual entrepreneurs may be treated as personal data.

What are the rules for processing personal data?

Personal data may generally be processed: (i) with the prior consent of the personal *data subject*; (ii) under an international treaty or pursuant to Russian law; (iii) for judicial purposes; (iv) for the purpose of the united web based portal of state and municipal services; (v) for the purpose of an agreement with the *data subject* or an agreement where the *data subject* is beneficiary or guarantor; (vi) for statistical or other scientific purposes (in which case, however, data must be anonymised); (vii) for the protection of the life, health or other legitimate interests of the *data subject*, in cases where obtaining their prior consent is impossible; (viii) for the protection of the data operator's or third parties' rights or for public purposes, if there is no breach of the *data subject's* rights and freedoms; (ix) for the purposes of mandatory disclosure or publication of personal data in cases directly prescribed by law; (x) in the context of professional journalistic, scientific, literary or other creative activities, if there is no breach of the *data subject's* rights and freedoms; or (xi) if such data were made publicly available by the *data subject* or under his/her instruction.

Are there any formalities to obtain consent to process personal data?

The OPD Law requires any consent to be in writing and that the consent is specific, informed and freely given. The OPD Law allows the consent to be collected in electronic form based on the electronic signature of the *data subject*.

The consent should include: (i) the surname, first name, patronymic, address of the *data subject* and information on the identity document of the *data subject* and his/her representative (if applicable); (ii) name and address of the data operator and/or third party processor; (iii) the purpose of the processing; (iv) a list of the relevant personal data to be processed; (v) a list of actions for which consent is given and a general description of methods of data processing used by the operator; (vi) the term of the consent and the procedure for its revocation; (vii) the surname, first name, patronymic and address of a person processing data at the request of the data operator (if applicable); and (viii) the signature of the *data subject*.

Sensitive Personal Data

What is sensitive personal data?

Under the OPD Law, sensitive personal data include nationality, racial or ethnic origin, political opinions, religious or philosophical beliefs, and the processing of data concerning health or sex life.

Criminal offence information is considered to be sensitive personal data that may be processed by state or municipal bodies only in cases set out in the Russian federal laws.

According to the OPD Law, biometric information is treated as a separate class of personal data with its own legal regime. Biometric personal data may be processed without the consent of the personal *data subject* thereto in connection with the administration of justice and other specific instances as stipulated by applicable laws.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed only if: (i) the *data subject* has provided his/her consent to the processing of personal data in writing; (ii) the personal data were made public by the *data subject*; (iii) it is required under an international treaty of the Russian Federation on readmission (i.e. return of immigrants); (iv) it is performed for the all-Russian population census; (v) it is performed under the laws on social support, employment or pensions; (vi) the data processing is necessary to protect the life, health and vitally important legitimate interests of the *data subject* or other individuals, provided that it is impossible to obtain the *data subject's* consent; (vii) it is carried out by a person who is engaged in professional medical activity for medical purposes and subject to medical confidentiality; (viii) it is performed by religious organisations or public societies on their members' personal data; (ix) it is necessary in connection with the ascertaining of rights or enforcement of rights of the *data subject* or third parties as well as for the administration of justice; (x) it is performed in accordance with Russian state security, anti-terrorist, transport safety, anti-corruption, law-enforcement, criminal investigation or criminal prosecution legislation; (xi) it falls under mandatory types of insurance, under the insurance legislation; and (xii) it is necessary for child adoption.

Processing of sensitive personal data (where it is permitted) shall be stopped immediately if the reasons for such processing are eliminated.

Are there any formalities to obtain consent to process sensitive personal data?

The formalities are the same as those for consent to process personal data (see above).

Scope of Application

What is the territorial scope of application?

The OPD Law does not contain any express provisions on its territorial effect. It is, therefore, likely to apply to processing of personal data in Russia and/or processing of personal data which relates to Russian citizens or residents regardless of where the data operator is established.

Who is subject to data protection legislation?

Russian law does not contain the concepts *data controller* and *data processor*. Instead, the OPD Law refers to the single concept of a "data operator", which is a person, state or municipal body that organises and/or carries out (alone or with other operators) the processing of personal data and also determines the purposes, content and actions of personal data processing (this definition somewhat combines the two definitions of *data controller* and *data processor* under the *Data Protection Directive*). There are, however, specific rules that apply when a third party processes personal data on behalf of the data operator.

The OPD Law applies to all data operators.

Are both manual and electronic records subject to data protection legislation?

The OPD Law applies to both manual and electronic records.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation for damage, including moral damages.

Fair processing information

No rules regarding *fair processing information* have been incorporated into the OPD Law.

Rights to access information

Data subjects may obtain their *subject access information* by a request to the personal data operators. A subject access request is free of charge. There are statutory exceptions where the *data subject's* right of access to his/her personal data may be restricted in accordance with federal laws.

Objection to direct marketing

Under the OPD Law, a *data subject* is entitled to revoke his/her consent to the processing of personal data for purposes of the direct marketing of goods, work or services.

Other rights

In certain cases, a *data subject* may request that the personal data operator rectify, block or delete personal data. In certain cases, a *data subject* may object to decisions being taken based solely on automatic processing of the *data subject's* personal data.

Security

Security requirements in order to protect personal data

The OPD Law only refers to the *general data security obligations* and does not contain any specific security requirements.

However, the Russian Government has adopted Resolution No. 1119, dated 1 November 2012, which implements measures and requirements in order to prevent any unauthorised access to personal data.

Specific rules governing processing by third party agents (processors)

Under Russian law an operator is allowed, with the consent of the *data subject*, to engage a third party to process personal data on the basis of an agreement, state or municipal contract or under the state or municipal legal act issued by the relevant authority (the "**Operator's Instruction**").

The Operator's Instruction must contain a list of processing actions performed by the third party processor, the purposes of such processing and the obligation of the third party processor to maintain confidentiality and ensure protection of personal data in compliance with the OPD Law.

Notice of breach laws

Data operators are required to notify *data subjects* and Roscomnadzor of breaches of the OPD Law if there is a request for confirmation of compliance with the OPD Law by Roscomnadzor. This notification obligation also applies to security breaches.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The OPD Law contains the following restrictions on *transborder dataflows*. Prior to the transborder transfer of personal data, a data operator must check whether the foreign jurisdiction to which the personal data are to be transferred provides adequate protection for the rights of *data subjects*. The transfer of personal data to a jurisdiction with adequate protection

is generally permitted, subject to the provisions of the OPD Law and any further restrictions and limitations in the Russian constitutional system.

There is no need to obtain a consent for transfer of personal data to the territory of states that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and to those states who are not parties to the Convention, but are named by Roscomnadzor as providing an adequate level of data protection. Please note that this applies to the consent for transborder transfer only; the general rules for processing under the OPD Law still apply and must be satisfied in relation to any transfer.

The transfer of personal data to a foreign jurisdiction which does not provide adequate protection of *data subjects'* rights may take place only: (i) with the prior written consent of the *data subject*; (ii) under an international treaty; (iii) under a Russian federal law, if it is required to protect the Russian constitutional system and ensure the defence of the country and security of the state; (iv) to ensure the safety of the transportation system; (v) in the context of the performance of an agreement with the *data subject*; or (vi) for the protection of the *data subject's* life, health and other vital interests when it is impossible to obtain their prior consent.

These conditions are broadly similar to the *standard conditions for transborder dataflow*.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no additional obligation to notify or obtain the approval of Roscomnadzor for *transborder dataflows*.

Use of binding corporate rules

No concept of *binding corporate rules* is used in the OPD Law.

Enforcement

Sanctions

Breaches may lead to administrative and civil liability, as well as to certain criminal sanctions for violations of privacy, which include fines. However, these sanctions do not include imprisonment.

Practice

The OPD Law has been updated several times since it was adopted in 2006. There is currently no established court or regulatory practice relating to the application of its provisions.

Enforcement authority

Roscomnadzor may impose administrative fines on a data operator and/or its officials.

ePrivacy | Marketing and cookies

National Legislation

ePrivacy laws

There are no specific ePrivacy laws but the OPD Law does contain provisions on direct marketing.

Cookies

Conditions for use of cookies

No concept of cookies is used in the OPD Law.

Regulatory guidance on the use of cookies

There is no official guidance on cookies from Roscomnadzor.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under the OPD Law, personal data processing for direct marketing purposes is only allowed with the prior consent of the *data subject*.

Conditions for direct marketing by e-mail to corporate subscribers

The OPD Law does not apply to corporate subscribers.

Exemptions and other issues

Consent can be revoked by the *data subject* at any time.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Under the OPD Law, personal data processing for direct marketing purposes is only allowed with the prior consent of the *data subject*.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The OPD Law does not apply to corporate subscribers.

Exemptions and other issues

Consent can be revoked by the *data subject* at any time.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Under the OPD Law, personal data processing for direct marketing purposes is only allowed with the prior consent of the *data subject*.

Conditions for direct marketing by fax to corporate subscribers

The OPD Law does not apply to corporate subscribers.

Exemptions and other issues

Consent can be revoked by the *data subject* at any time.

Singapore.

General I Data Protection Laws

National Legislation

General data protection laws

The Personal Data Protection Act 2012 ("**PDPA**").

In addition, certain sector-specific laws such as the Banking Act (Cap. 19) and the Securities and Futures Act (Cap. 289) include provisions relating to the protection of certain personal data (such as particulars of accounts of customers of a bank). Companies in industries such as telecommunications may also be subject to Codes of Practice which impose data protection-related obligations. This summary does not consider these sector-specific laws and codes. Further, common law duties of confidentiality may also apply under certain circumstances.

Entry into force

The PDPA was finalised in November 2012. Although the PDPA was enacted on 2 January 2013, the majority of its positions have yet to come into force. The main provisions relating to the Do Not Call Register (see below) are expected to come into force in early 2014 (although provisions about the establishment of the Do Not Call Register came into force on 2 January 2013). The main provisions relating to the collection, use and disclosure of personal data are expected to come into force in mid 2014.

However, the remainder of this summary has been prepared as if the PDPA was in fact in force in full.

National Regulatory Authority

Details of the competent national regulatory authority

The Personal Data Protection Commission (the "**Commission**").

http://www.pdpc.gov.sg

At the date of publication of this summary the Commission had just been established and was located at a temporary address. The Commission is expected to move to a permanent location during the course of 2013.

The Info-communications Development Authority of Singapore has been appointed to help administer compliance with the PDPA.

Notification or registration scheme and timing

The PDPA does not include a general notification or registration scheme.

Exemptions

Not applicable.

Appointment of a data protection officer

An organisation must appoint one or more individuals to be responsible for that organisation's compliance. The contact details of at least one such individual must be made available to the public.

Personal Data

What is personal data?

Personal data is data, whether true or not, about an individual who can be identified: (i) from that data; or (ii) from that data and other information to which the organisation has or is likely to have access. This is similar to the *standard definition of personal data*.

Business contact information (unless provided solely for personal purposes) is largely exempt from the provisions of the PDPA.

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

The PDPA regulates the collection, use and disclosure of personal data by Organisations (as defined below). The main provisions governing the collection, use and disclosure of personal data will not apply to any individual acting in a personal or domestic capacity, or to any public agencies.

The collection, use and disclosure of personal data is permitted where: (i) the individual has consented; or (ii) those activities are required by law. Alternatively, the collection, use or disclosure of personal data can be carried out without consent if a condition in Schedules 2, 3 and 4 to the PDPA respectively is satisfied. There are different conditions depending on whether the organisation is collecting, using or disclosing the relevant personal data. Those conditions are similar to the *standard conditions for processing personal data* but are much more extensive.

There is an overriding obligation on the organisation to collect, use and disclose personal data in a manner a reasonable person would consider appropriate in all the circumstances. The PDPA includes obligations to ensure that certain personal data it holds is accurate and to retain personal data for no longer than necessary. The organisation must also implement appropriate data protection policies and processes and make available information on the same.

Are there any formalities to obtain consent to process personal data?

Consent can be expressly given or deemed to be given. Express consent will only be valid if the individual has been provided with certain information about the purpose of collection and the consent cannot be made a condition of the provision of a product or service (beyond what would be reasonable for the provision of that product or service).

Deemed consent will arise when an individual voluntarily provides personal data for a particular purpose and it is reasonable for such provision of personal data to take place.

There is no general requirement that consent is in writing though this may be necessary when marketing to someone on the Do Not Call Register (see below).

Sensitive Personal Data

What is sensitive personal data?

The PDPA does not include a separate category of sensitive personal data.

Are there additional rules for processing sensitive personal data?

Not applicable.

Are there any formalities to obtain consent to process sensitive personal data?

Not applicable.

Scope of Application

What is the territorial scope of application?

The PDPA does not contain express provisions on territorial effect. Generally, it is likely to be interpreted as applying as long as the collection, use and/or disclosure of personal data takes place within Singapore, even if any remaining part(s) of the data processing takes place somewhere else in the world.

Who is subject to data protection legislation?

The PDPA applies to any individual, company, association or body of persons, corporate or unincorporated, whether located in or outside Singapore ("**Organisations**").

It also contains the concept of data intermediaries (a concept similar to that of *data processors*). Where a data intermediary processes personal data under a contract in writing with an organisation and for the purposes of that organisation, it will be largely exempt from the PDPA and only subject to the security and retention obligations therein.

Are both manual and electronic records subject to data protection legislation?

Data is not specifically defined in the PDPA to include manual and electronic records, however, it is likely that the intention is that both manual and electronic records are subject to the PDPA.

Rights of Data Subjects

Compensation

A person who suffers loss as a result of breach of the rules on collection, use and disclosure, as well as access to, correction and care of personal data, shall have a right of action in civil proceedings in court. The court may award damages, injunctions or other remedies as it sees fit.

Fair processing information

Organisations should provide individuals with details of the purposes for which their personal data is collected, used or disclosed. This obligation arises when seeking express consent from them or when the use or disclosure of their personal data is for a purpose other than that for which it was originally envisaged and notified to the individual.

Individuals can also request contact details for an organisation's data protection officer.

Rights to access information

Individuals have a right of access to their personal data and to details of the way in which their personal data has been or may have been used or disclosed within one year prior to the request of access. There are a wide range of exemptions to this right, for example where there would be disclosure of personal data about another individual. Additional details about this right, including the fee and timetable to respond, may be set out in further regulations in due course.

Objection to direct marketing

There is no general right to object to direct marketing. However, individuals can withdraw consent to the collection, use and disclosure of their personal data at any time and there are specific direct marketing restrictions under the Do Not Call Register (see below).

Other rights

Individuals have a right to ask organisations to correct their personal data. Individuals also have a right, on reasonable notice to the organisation, to withdraw their consent to the collection, use or disclosure of their personal data, in which case the organisation must inform the individual of the likely consequences of such withdrawal of consent and cease collecting, using and disclosing that individual's personal data except to the extent required or authorised under law.

Security

Security requirements in order to protect personal data

Organisations must make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks.

Specific rules governing processing by third party agents (processors)

Organisations are responsible for any processing carried out by their data intermediaries.

Data intermediaries who process personal data under a contract in writing with an organisation and for the purposes of that organisation will be largely exempt from the PDPA and only subject to the security and retention obligations therein.

Notice of breach laws

No.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Organisations may only transfer personal data outside of Singapore in accordance with certain prescribed requirements to ensure that data remains subject to an adequate level of protection that is comparable to the protection allowed under the PDPA. At the date of publication of this summary, no such requirements have been prescribed, though it is expected that there will be regulations prescribed.

Notification and approval of national regulator (including notification of use of Model Contracts)

The Commission has the power to exempt an organisation from any prescribed requirements.

Use of binding corporate rules

The Commission's "Proposed Positions for Regulations under the PDPA" (the "Proposed Regulations") recommends that where contractual arrangements are not suitable for intra-corporate transfers of data, *binding corporate rules* would be an acceptable avenue to safeguard personal data transferred overseas. This set of Proposed Regulations is, at the time of publication, in the consultation stage and may be subject to further amendments.

Enforcement

Sanctions

The Commission has a range of powers under the PDPA including directing an organisation to: (i) stop collecting, using or disclosing personal data; (ii) destroy personal data; (iii) comply with any directions from the Commission; and (iv) pay a financial penalty of up to S$1million.

The PDPA contains various criminal offences including: (i) unauthorised access to, or alteration of, personal data; (ii) alteration, falsification, concealment or destruction of personal data with the intent of evading an access or correction request; (iii) obstructing or impeding the Commission; and (iv) knowingly or recklessly making false statements to the Commission. The penalty for an offence includes fines of up to S$100,000 and imprisonment for up to three years.

There are separate penalties for breach of the Do Not Call Register (see below).

Practice

The majority of the PDPA has not come into force yet so there is no established enforcement practice.

Enforcement authority

The Commission will issue directions which can be enforced in the District Court. The District Court will have jurisdiction to try any offence under the PDPA and shall have power to impose the full penalty or punishment in respect of that offence.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The PDPA contains provisions relevant to telephone and fax marketing. These rules require the Commission to set up a Do Not Call Register. The rules apply to "specified messages" which are messages the purpose of which is to offer or advertise goods, services, land or investment opportunities. There are a number of exemptions to the term "specified messages" set out in the schedule to the PDPA including messages sent to a business for a purpose of that business. The provisions relating to the establishment of the Do Not Call Register have come into force but the actual restrictions on telephone and fax marketing are not yet effective.

The rules relevant to direct marketing by email, text and multi-media marketing are generally set out in the Spam Control Act (Cap 311A) (the "**SCA**").

Cookies

Conditions for use of cookies

Consent is not needed for cookies that do not collect personal data, and may not be needed where the use of cookies to collect data pertains to internet activities which the individual has clearly requested. Where an individual has configured his or her browser to accept certain cookies but reject others, consent may be deemed to have been given. Where cookies for behavioural targeting actually collect personal data, the individual's consent is required.

Regulatory guidance on the use of cookies

The publication titled "Advisory Guidelines on Selected Topics" made available by the Commission clarifies that the PDPA applies to the collection, use, or disclosure of personal data using cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

It is only possible to send commercial e-mails "in bulk", each addressed to individual or corporate subscribers, if they consent.

Conditions for direct marketing by e-mail to corporate subscribers

It is only possible to send commercial e-mails "in bulk", each addressed to individual or corporate subscribers, if they consent.

Exemptions and other issues

It is also possible to send such bulk e-mail if: (i) complies with particular requirements set out in the SCA, including a labelling requirement and a requirement to provide an unsubscribe facility; (ii) the subscriber does not "unsubscribe"; and (iii) the relevant e-mail address was not obtained through dictionary attack or address harvesting.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

No person shall send a specified message to a Singapore telephone number that is listed on the Do Not Call Register unless the relevant subscriber or user has given consent.

Marketing by text message is subject to these rules and is also subject to the rules on marketing by e-mail above.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

No person shall send a specified message to a Singapore telephone number that is listed on the Do Not Call Register unless the relevant subscriber or user has given consent.

Marketing by text message is subject to these rules and is also subject to the rules on marketing by e-mail above.

Exemptions and other issues

Any consent must be clear and unambiguous and in writing or other similar medium. Consent cannot be made a condition to the supply of goods, services, land, interests, or opportunities beyond what is reasonable for purposes of the same.

The person sending the specified message must: (i) identify the person who sent or authorised the sending of that message; (ii) include contact details; and (iii) contain such other information as may be set out by regulation from time to time. Where the specified message is a voice call, the person making the call must not conceal or withhold their calling line identity.

These obligations will come into force on a date to be prescribed.

Marketing by text message is subject to these rules and is also subject to the rules on marketing by e-mail above.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

The same as for telephone marketing (see above).

Conditions for direct marketing by fax to corporate subscribers

The same as for telephone marketing (see above).

Exemptions and other issues

The same as for telephone marketing (see above).

Slovakia.

Contributed by Kinstellar, s.r.o.

General | Data Protection Laws

National Legislation

General data protection laws

Act No. 428/2002 Coll. on the Protection of Personal Data dated 3 July 2002, as amended by Act No. 583/2008 Coll. (the "**Act**" or the "**DPA**") has implemented the *Data Protection Directive*.

Entry into force

The Act came into force on 1 September 2002 (the amending Act No. 583/2008 came into force on 1 January 2009).

National Regulatory Authority

Details of the competent national regulatory authority

Office for the Protection of Personal Data (*Úrad na ochranu osobných údajov*) (the "**Office**")
Hraničná 12
SK-820 07 Bratislava 27
Slovakia

http://www.dataprotection.gov.sk

Notification or registration scheme and timing

Under the Act there are two types of registration scheme:

General Registration Scheme: This applies to all information systems where personal data are processed wholly or partly by automatic means (subject to the exemptions listed in the section entitled "Exemptions" below). The general registration scheme does not require any approval by the Office. The processing of data may commence upon filing the necessary information with the Office.

Special Registration Scheme: This applies to all information systems in which the *data controller* processes: (i) at least one of the *standard types of sensitive personal data*, and this sensitive personal data is transferred to a non-EU country that does not ensure an adequate level of protection; (ii) personal data without the consent of the *data subject* where such processing is aimed at protecting the legally protected rights and interests of the *data controller* or a third party; or (iii) biometric data, except for DNA analysis, for the purposes of recording entries into highly protected facilities and if so required for the internal interests of the *data controller*. In the case of the special registration scheme, prior approval by the Office is necessary before the processing may begin.

The *data controller* must register the information system under the general registration scheme and under the special registration scheme, in both cases prior to starting to process the data. There is no charge for registration.

Exemptions

The general registration scheme does not apply to information systems which: (i) are subject to special registration; (ii) are supervised by a responsible person (data protection officer) designated by the *data controller* in writing, who supervises data protection under the Act; (iii) contain data on individuals (including data on their close persons) which are processed for the purposes of carrying out the rights or obligations of the *data controller* under employment or membership relationships; (iv) contain data on membership in trade unions, political parties or religious organisations, if such data are used solely for internal purposes of these organisations; and (v) contain data which are necessary for exercising rights or observing obligations under a separate law, or which are processed on the basis of a separate law.

No exemptions apply in the case of the special registration scheme.

Appointment of a data protection officer

Under the Act, if the *data controller* employs more than five persons, he is obliged to authorise a data protection officer in writing to carry out internal supervision and these persons shall supervise compliance with the Act in the processing of personal data. Employing a data protection officer also provides an exemption to the notification requirement under the general registration scheme.

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*.

In practice, the Office often interprets the definition of personal data more narrowly and only considers that information (a set of information) can be personal data if the individual is either identified or identifiable based on such particular (set of) information (and not other information that might be held by the *data controller* now or in the future).

This interpretation is demonstrated, *inter alia*, from the Report on Data Protection in the Slovak Republic issued by the Office. However, this approach has not been tested by the Slovak courts yet. As the interpretation of the Office does not correspond to the *Opinion on Personal Data* and departs from the statutory definition under the DPA, it remains highly controversial.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. The Slovak DPA also authorises, subject to certain conditions, the processing of personal data for artistic or journalistic purposes (to the extent it does not interfere with the right to privacy), direct marketing purposes or where the personal data have already been published.

In practice, it should be noted that processing based on the legitimate interests test is subject to the prior special registration with (approval by) the Office.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

Generally, there are no formalities for obtaining consent from *data subjects*. The consent to process personal data may be verbal or in writing, however, in case of doubt, the burden of proof lies on the *data controller*. The *data controller* must be able to show, in particular, details of: (i) who gave the consent; (ii) to whom it was given; (iii) for what purpose it was given; (iv) the list or scope of personal data; (v) the term of validity of the consent; and (vi) the terms of its withdrawal.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes: (i) the *standard types of sensitive personal data*; (ii) national identification number; (iii) information on psychological identity or psychological ability to perform work; (iv) biometric information; and (v) information about breaches of criminal or civil law and the enforcement of the respective judgments.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if conditions which substantially follow the *standard conditions for processing sensitive personal data* are met. However, these are interpreted very restrictively in practice.

Biometric data can be processed if *data subjects* have agreed to such processing in a written form, or under a special law whereby the data processing by the *data controller* stems from such law. This restriction does not apply where a special registration requirement in respect of the biometric data processing applies (in such case, the biometric data processing is approved by the Office).

Are there any formalities to obtain consent to process sensitive personal data?

Consent from *data subjects* to the processing of sensitive personal data must be in writing.

Scope of Application

What is the territorial scope of application?

The Act applies the *standard territorial test*. Where the *data controller* is not established in an EU Member State but has a representative in Slovakia, such representative is bound by the same obligations as the *data controller*.

Who is subject to data protection legislation?

The Act makes a distinction between *data controllers* and *data processors*. Both are responsible for compliance with the Act, though to different extents.

If a separate law regulates the purposes and means of processing of personal data, the *data controller* is an entity which is designated by such law to fulfil the purposes of processing or satisfying the conditions set out by the law. The same also applies if so determined by Community law.

Are both manual and electronic records subject to data protection legislation?

Yes, both manual and electronic records are subject to data protection legislation.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation (claim for damages under the general civil law) if they suffer damage due to a breach of statutory obligations set forth in the DPA.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. This includes: (i) the identity of the person collecting personal data; (ii) information on whether the provision of personal data is voluntary or compulsory; (iii) third parties or other recipients that may have access to personal data; (iv) the form of publication, should such data be published; (v) the non-EU countries to which the data may be transferred; and (vi) an explanation of the rights of *data subjects*.

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. The *data subject* may only be required to pay the cost of copying and mailing the information about: (i) the data undergoing processing; and (ii) information as to their source.

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing his personal data for direct marketing purposes. The *data controller* must then cease such processing without delay after the relevant request has been made.

Other rights

Data subjects have the right to request from the *data controller* (subject to certain exceptions) the correction of incorrect and out-of-date personal data that are the subject of processing, deletion of personal data after the purpose of processing is achieved and deletion of personal data processed in breach of the Act.

Data subjects are entitled to object to the processing of their data in certain cases where the Act does not require the consent of a *data subject*, where such processing represents an unjustified interference with their rights or their interests protected by law.

Data subjects have the right not to be subject to a decision that produces legal effects concerning them or significantly affecting them which is based solely on automated processing of data, and the right to reject the cross-border transfer of their personal data to a third country which does not have an adequate level of protection.

Security

Security requirements in order to protect personal data

Both the *data controller* and the *data processor* are responsible for compliance with the *general data security obligations*. When taking the appropriate measures, the following must be taken into consideration: (i) the technical means that may be used; (ii) the extent of risks that may negatively impact the safety or functionality of the information system; and (iii) the confidentiality and importance of data that are processed. In certain cases, the technical and organisational measures are to be implemented by the *data controller* and the *data processor* in the form of a security project.

Specific rules governing processing by third party agents (processors)

A *data controller* may authorise a *data processor* to carry out the processing of personal data by way of a written contract or a written instruction (accepted by the *data processor*).

Notice of breach laws

The data protection officer must inform the *data controller* of each breach of the DPA. If the *data controller* does not, without undue delay, remedy the breach, the data protection officer must notify the Office of such breach.

Effective as of 1 November 2011, specific notice of breach of laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Transfer of data to jurisdictions outside of the EU to non-*whitelisted countries* is subject to certain restrictions and generally depends on whether or not the other country offers an adequate level of protection.

The DPA does not exclude the possibility that the assessment of adequacy can be made by the *data controller*, with the Office having the right to make the final decisions in this respect if doubts arise. In such case, the only conditions that must be satisfied relate to the fact that *data subjects* must be adequately informed.

If the destination country does not offer an adequate level of protection, cross-border transfer of personal data is allowed if, in principle, such transfer satisfied the *standard conditions for transborder dataflow*. However, consent to any transborder dataflow must be in writing.

It should also be noted that the DPA treats the EEA States (Norway, Liechtenstein and Iceland) as third countries for the purposes of transborder dataflow restrictions.

Notification and approval of national regulator (including notification of use of Model Contracts)

A notification to and approval by the Office is required in respect of a transborder dataflow between a *data controller* based in Slovakia and a *data processor* based outside of the EU. In practice, the Office takes the view that such notification and approval are required only where the *data processor* is based in a third country not ensuring an adequate level of protection. However, such distinction does not clearly follow from the wording of the relevant provisions of the DPA.

It should be noted that the approval is granted by the Office only where the agreement between the *data controller* and *data processor* conforms to *Model Contracts*. Based on the non-binding guidance issued by the Office, the *Model Contracts* are not required for *transborder dataflows* covered by the safe harbor regulations.

Use of binding corporate rules

The DPA, as is currently in force, does not give a sufficiently clear legal ground for *data controllers* to rely on the *binding corporate rules*. However, Slovakia is part of the mutual recognition club for *binding corporate rules* and it seems that the Office supports and accepts *binding corporate rules* as prospectively sufficient safeguards of *data subjects'* rights in the context of *transborder dataflows*.

Enforcement

Sanctions

The Office may impose: (i) a penalty of up to approximately EUR 332,000 for the processing of personal data in breach of the Act or other serious offences; (ii) a penalty of up to approximately EUR 166,000 for breach of obligations related to liquidation of personal data or certain other major offences; (iii) a penalty of up to approximately EUR 99,600 for breach of the obligation related to registration of information systems, or certain other minor offences; or (iv) a penalty of up to approximately EUR 33,200 for other named offences.

The Slovak Criminal Code provides for criminal sanctions for the unauthorised manipulation of personal data including imprisonment or a fine. Unauthorised breach of the right to personal integrity and privacy can also trigger responsibility under the Slovak Civil Code.

Practice

According to the most recent Report on Data Protection in the Slovak Republic issued by the Office, between 1 January 2009 and 31 December 2010 the number of complaints received by the Office was 549 (339 of which were against entities from the private sector). In the same period, the Office issued 305 remedy measures and imposed financial penalties in 40 cases amounting to EUR 88,024.19.

According to the statistics of the General Prosecutor's Office of the Slovak Republic, six persons were prosecuted, four were accused and four condemned in connection with the crime of unauthorised manipulation of personal data under the Slovak Criminal Code in 2011.

Enforcement authority

The Office has broad powers to take various enforcement actions, including the power to issue remedy measures imposing obligations upon the *data controller* or *data processor* and the power to impose penalties. The Office also issues opinions or statements regarding both public and private data protection issues.

Prosecutions for criminal offences are brought by the prosecutor's offices before the Slovak courts, which can impose criminal sanctions.

Civil law remedies can be sought by the affected individuals before the Slovak courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Act on Electronic Communications of 14 September 2011 (the "**ECA**") implemented Article 13 of the *Privacy and Electronic Communications Directive*. Direct marketing is subject to Section 62 of the ECA, which came into force on 1 November 2011.

The newly passed ECA implemented the amendments to the *Privacy and Electronic Communications Directive* introduced by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

According to the newly passed ECA, cookies may be used only if the user concerned has given his consent based on clear and comprehensive information about the purpose of processing. The ECA provides an exception from the consent requirement for law enforcement authorities and other state authorities. The ECA expressly refers to the use of browser settings as means to obtain the consent. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide the information society service explicitly requested by the user.

Regulatory guidance on the use of cookies

There is no regulatory guidance for the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing by e-mail is authorised, subject to the subscriber's prior consent. Consent already given can be withdrawn at any time.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing by e-mail is authorised, subject to the subscriber's prior consent. Consent already given can be withdrawn at any time.

Exemptions and other issues

Since 1 April 2006 the *similar products and services exemption* has been available. The sending of e-mail for purposes of direct marketing that does not specify the identity of the sender or a valid address to which the recipient may send a request seeking termination of such communication is prohibited. The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing by telephone is authorised, subject to the prior consent of the individual subscriber. Consent already given can be withdrawn at any time.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Direct marketing by telephone is authorised, subject to the prior consent of the corporate subscriber. Consent already given can be withdrawn at any time.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax is authorised, subject to the prior consent of the individual subscriber. Consent already given can be withdrawn at any time.

Conditions for direct marketing by fax to corporate subscribers

Direct marketing by fax is authorised, subject to the prior consent of the corporate subscriber. Consent already given can be withdrawn at any time.

Exemptions and other issues

No exemptions apply.

Slovenia.

Contributed by Schönherr Rechtsanwälte GmbH

General | Data Protection Laws

National Legislation

General data protection laws

The current Slovenian Personal Data Protection Act (*Zakon o varstvu osebnih podatkov*, UL RS No. 86/2004 et seq, "**ZVOP-1**") replaced the previous Personal Data Protection Act (UL RS No. 59/1999, "**Old ZVOP**") and implemented the *Data Protection Directive*.

Entry into force

The Old ZVOP, which first transposed the *Data Protection Directive* into Slovenian law, entered into force on 7 August 1999. The new ZVOP-1 entered into force on 1 January 2005 and the latest amendments to the ZVOP-1 entered into force on 28 July 2007 by implementation of the Act on Changes and Amendments to the Personal Data Protection Act (UL RS no. 67/2007).

National Regulatory Authority

Details of the competent national regulatory authority

The Information Commissioner (*Informacijski pooblascenec*) (the "**Commissioner**")
Vošnjakova 1
p.p. 78
SI-1000 Ljubljana
Slovenia

www.ip-rs.si

Notification or registration scheme and timing

The *data controller* must notify the Commissioner before carrying out any wholly or partly automatic processing operation or before adding a new category of information to the system.

There is no charge for notification. No approval or consent is required. The notification must occur no later than 15 days prior to commencing data processing. Any changes with respect to the method, purpose or scope of the data processing have to be notified to the Commissioner within eight days of the adoption of any such changes.

Exemptions

The requirement to notify the Commissioner and keep details of the processing undertaken do not apply to processing of personal data: (i) by political parties, unions, associations or religious communities if the personal data being processed relates to the members of such parties, unions, associations or communities; (ii) by the media for purposes of informing the public; or (iii) by *data controllers* that have 50 or less full time employees.

However, the exemption for *data controllers* with 50 or less full time employees does not apply to filing systems kept by *data controllers* in the public sector, notaries public, attorneys, detectives, bailiffs, private security providers, private healthcare workers, healthcare providers, and to *data controllers* that keep filings systems containing sensitive personal data and processing of sensitive personal data as a part of their registered activity.

Appointment of a data protection officer

There is no obligation to appoint a data protection officer as such, but *data controllers* must specify the persons who are responsible for individual data collections/filing systems and specify the persons who, due to the nature of their work, are permitted to process certain types/kinds of personal data.

Personal Data

What is personal data?

According to the ZVOP-1 personal data is any data relating to an individual (an identified or identifiable natural person to whom personal data relates), 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 or disproportionate effort or require a large amount of time. This definition is therefore closely based on the *standard definition of personal data*.

The ZVOP-1 also has a limited number of provisions that apply to deceased individuals.

Is information about legal entities personal data?

No. The ZVOP-1 only applies to information about individuals. Data on sole traders and partnerships is not classified as personal data, especially when involving business transactions.

What are the rules for processing personal data?

As a general rule, personal data may be processed if: (i) the processing of personal data and the personal data being processed are provided for by statute; or (ii) if personal consent of the *data subject* has been given for the processing of certain personal data. The ZVOP-1 also provides a number of other statutory bases that are broadly similar to the *standard conditions for processing personal data*.

However, in considering whether these conditions apply, a distinction is drawn between the public and private sectors with processing in the public sector generally needing to be specified by law.

Are there any formalities to obtain consent to process personal data?

The individual must be informed in advance in writing or in another appropriate manner of the purpose of the processing of personal data. It is advisable to obtain consent in writing as the Commissioner may demand proof that such consent has actually been given.

Sensitive Personal Data

What is sensitive personal data?

Under the ZVOP-1, sensitive personal data includes: (i) the *standard types of sensitive personal data*; (ii) information about criminal records and minor offences; and (iii) biometric information if it can be used to identify sensitive personal data about a *data subject*.

The ZVOP-1 also has a range of additional restrictions that apply to video surveillance, biometric information, access control information and connecting systems.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. In addition, when processing sensitive data the data must be labelled and protected so as to prevent unauthorised access. Transfer of sensitive data is deemed adequately secure if the data are encrypted so they are illegible and unrecognisable during transfer.

Information about criminal records is kept by the Ministry of Justice and may be given to the court, state prosecutor's office and official bodies for internal affairs as well as to state authorities, legal persons and private employers upon a written request in the case of having legitimate interest based on law.

Are there any formalities to obtain consent to process sensitive personal data?

Consent from a *data subject* must be explicit and, as a general rule, given in writing.

Scope of Application

What is the territorial scope of application?

The ZVOP-1 applies the *standard territorial test*.

Who is subject to data protection legislation?

The *data controller* is primarily responsible for compliance with the ZVOP-1. *Data processors* are only subject to the data security obligations in the ZVOP-1. Generally, ZVOP-1 does not apply to the processing of personal data performed by individuals exclusively for personal use, family life or other domestic needs.

Are both manual and electronic records subject to data protection legislation?

Yes. The ZVOP-1 applies to data: (i) subject to automated processing; or (ii) which is manually processed but forms part of a filing system or is intended for inclusion in a filing system.

Rights of the Data Subjects

Compensation

The right to compensation has not been directly implemented by the ZVOP-1. However, the *data subjects* have a right to compensation if they suffer damage according to the general provisions of the Code of Obligations (*Obligacijski zakonik*, UL RS, no. 97/2007) (the "**OZ**"). In accordance with the Art. 131 OZ, any person that inflicts damage on another shall be obliged to reimburse it, unless it is proved that the damage was incurred without the culpability of the former person (general principles of reimbursement of damages).

Fair processing information

Under the ZVOP-1, a *data controller* must provide the *fair processing information* to *data subjects*. The principle of legality and fairness must be upheld and requires a *data controller* to communicate to the *data subject* information on: (i) the data recipient or the type of data recipients of his personal data; (ii) whether the collection of personal data is compulsory or voluntary, and the possible consequences if the *data subject* will not provide data voluntarily; and (iii) the information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

There is no special requirement for the *fair processing information* to be provided in the local language. Nevertheless, the rules of administrative procedure as well as the rules on the public use of Slovene language will apply and, therefore, require the use of Slovenian in the provision of the *fair processing information*.

Rights to access information

Data subjects may obtain their *subject access information* by written request or orally for the record to *data controllers*. There is no charge for making a request. The *data controller* may only charge the *data subject* material costs for the transcription, copying and written certificate according to a pre-specified tariff.

The *data controller* must provide access within 15 days from when it received the request by a *data subject* or inform the *data subject* as to why his request was denied. A request may be filed every three months, or for sensitive personal data, every month.

Objection to direct marketing

A *data subject* may at any time in writing or in another agreed manner request that the *data controller* permanently or temporarily cease to use his personal data for the purpose of direct marketing. The *data controller* shall be obliged within 15 days to prevent as appropriate the use of personal data for the purpose of direct marketing, and within the subsequent five days to inform in writing or another agreed manner the *data subject* who so requested. The costs of all actions of the *data controller* in relation to such request shall be borne by the *data controller*.

Other rights

All persons shall have the right to ask the court or any other relevant authority to order that action that infringes the inviolability of the human person, personal and family life or any other personal right cease (this applies also to personal data), that such action be prevented or that the consequences of such action be eliminated (Art. 134 OZ).

Furthermore, the *data subject* may ask the *data controller* to change and/or amend incomplete, incorrect or out of date personal data and to erase personal data which have been collected illegally. The *data controller* must change and/or amend the personal data if the *data subject* proves that personal data is incomplete, incorrect or outdated. On request of the *data subject*, the *data controller* must inform all the users of the personal data of the respective changes.

Security

Security requirements in order to protect personal data

Data controllers must comply with the *general data security obligations*. In addition *data controllers* shall prescribe in their internal acts the procedures and measures for security of personal data and must specify the persons responsible for individual filing systems and the persons who, due to the nature of their work, can process individual personal data.

In processing sensitive data, the data must be labelled and protected so as to prevent unauthorised access. Transfer of sensitive data is deemed adequately secure if the data are encrypted so they are illegible and unrecognisable during transfer.

Specific rules governing processing by third party agents (processors)

Data processors are only authorised to carry out activities within the scope of the authorisation granted by the *data controller* and may not process personal data for any other purpose. Mutual rights and obligations shall be arranged by contract, which must be concluded in writing and must also contain an agreement on the procedures and measures pursuant to *general data security obligations*. The *data processor* must return the personal data it is processing at the end of the relationship.

Notice of breach laws

The ZVOP-1 does not contain any obligation to inform the Commissioner or *data subjects* of a security breach.

Additional obligations apply to public communication services under the ZEKom-1 (defined below). The person providing such services must: (i) immediately inform the Agency of any breaches; and (ii) notify, without unjustified delay, the respective subscriber or individual of the breach, if it is probable that the breach will detrimentally affect their personal data and privacy. Exceptions apply when adequate protective measures have been used.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

Transfers of personal data outside of the EEA are permitted if: (i) provided by statute or binding international treaty; (ii) made with the *data subject's* consent; (iii) necessary for the performance of a contract relating to the *data subject*; (iv) necessary to protect the vital interests of the *data subject*; or (v) made from a public register.

Transfer to third countries is also admissible if the respective third country is listed on the white list (currently, only Switzerland and Croatia have been put on the Slovene white list) or are part of the "Safe Harbour" list.

Notification and approval of national regulator (including notification of use of Model Contracts)

In all other cases, the exporter of personal data has to acquire the approval of the Commissioner in order to be allowed to export personal data to a country outside of the EEA. The approval is issued if the Commissioner establishes that a sufficient level of protection is ensured for the transferring of personal data respectively for the *data subjects* to which this data relates.

If the export agreement is identical to the *Model Contracts*, the Commissioner will approve it "automatically" and will not check the content of the agreement. If the export agreement deviates from the *Model Contracts*, it would be checked thoroughly (which will increase the time necessary for the approval to be issued).

Use of binding corporate rules

Yes. However, the use of *binding corporate rules* must be approved by the Commissioner. Slovenia is part of the mutual recognition club for *binding corporate rules*.

Enforcement

Sanctions

As already indicated (see "Compensation" above), a *data subject* who suffered damages due to breaches of law with regard to the collection and processing of his personal data may claim damages from the *data controller* (or other responsible person) on the basis of OZ.

Irrespective of the availability of civil damages, the Commissioner may impose monetary penalties in cases where there has been a breach of the provisions of the ZVOP-1, ranging from EUR 4,170 to EUR 12,510 for legal persons and entrepreneurs, from EUR 830 to EUR 2,080 for the responsible person of such legal person and from EUR 200 to EUR 830 for individuals.

The most severe violations of personal data privacy (such as misuse of personal data collected on the basis of a statutory provision or computer hacking) may constitute a criminal offence for which individuals may face imprisonment of up to one year (officials who have committed such acts by abusing their authority may face imprisonment of up to five years). Legal persons may face monetary fines of up to approximately EUR 500,000.

Practice

In 2010, the Commissioner initiated 276 inspection proceedings due to suspected violation of the ZVOP-1 in the private sector. As a result, 179 violation procedures and 35 monetary penalties were imposed on legal persons or their responsible persons due to violation of the ZVOP-1.

The Commissioner has actively encouraged the education of the public on the fundamental rights giving rise to the protection of personal data and regularly appears in the public media and frequently publishes education pamphlets as well as informative memoranda relating to topics connected with personal data protection (i.e. article on the implications of membership in certain internet-based social networks).

Enforcement authority

The Commissioner has the power to: (i) issue enforcement notices, such as to order the elimination of irregularities or deficiencies; (ii) order the prohibition of processing of personal data; and (iii) order the prohibition of the transfer of personal data to third countries or foreign recipients. The Commissioner also has the power to fine the violators of the ZVOP-1. The Slovenian Public Prosecution may bring charges against natural and legal persons for criminal offences connected with personal data privacy (see also "Sanctions" above).

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Slovenian ePrivacy laws are contained in: (i) the ZVOP-1; (ii) an amendment to the Slovenian Consumer Protection Act (Zakon o varstvu potrošnikov, UL RS No. 98/2004, 126/ 2007, 86/2009, 78/2011) (the "**ZVPot**"); and (iii) the new

Slovenian Electronic Communications Act (Zakon o elektronskih komunikacijah, UL RS No. 109/2012) (the "**ZEKom-1**"), entering into force on 15 January 2013 and implementing the *Privacy and Electronic Communications Directive*. and, respectively, the *Citizens' Rights Directive*. The public authority entrusted with the supervision of the effective execution of the respective provisions of ZEKom-1 is the Slovenian Electronic Communications Agency (Agencija za Posto in Elektronske Komunikacije), renamed under the new ZEKom-1 to the Agency for Communicational Networks and Services of the Republic of Slovenia (Agencija za komunikacijska omrežja in storitve Republike Slovenije) (the "**Agency**"). Until 30 June 2013 the Government of the Republic of Slovenia must amend the Act on the establishment of the Agency to the new provisions of ZEKom-1.

Cookies

Conditions for use of cookies

The new ZEKom-1 contains specific cookies regulations, implementing the *Citizens' Rights Directive*. Use of cookies is only allowed if the subscriber or user has given his or her consent, having been provided with clear and comprehensive information on the *data controller* and on the purpose of processing of this data in accordance with the ZVOP-1. An exception is provided: (i) where such use is necessary for the transfer of the message by means of the electronic communication network; or (ii) if it is necessary for the provision of an information society service requested by the subscriber or the user. Consent by the user may be given based on browser settings where technically feasible and effective.

Regulatory guidance on the use of cookies

There is no regulatory guidance on the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing by e-mail is governed by the sector-specific ZEKom-1 and is permitted only with the subscriber's or user's prior consent.

Conditions for direct marketing by e-mail to corporate subscribers

Direct marketing by e-mail is governed by the sector-specific ZEKom-1 and is, in principle, permitted only with the prior consent of the addressee.

Exemptions and other issues

ZEKom-1 allows direct marketing by e-mail where the *similar products and services exemption* applies. The sending of e-mail for purposes of direct marketing which: (i) disguises or conceals the identity of the sender on whose behalf the communication is made; or (ii) is sent without a valid address to which the recipient may respond, is prohibited. The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Pursuant to the ZVOP-1, the utilisation of personal telephone numbers for the purposes of direct marketing is, in principle, permitted, if the *data controller* has obtained the telephone number of the individual either: (i) from publicly available sources; or (ii) in the course of the lawful conduct of the business activity. The person using the individual's telephone number for the purpose of direct marketing is further obliged to inform the individual of his right to request that such communication ceases at any time, permanently or temporarily.

However, under the ZEKom-1, the use of direct marketing such as non-automated (speaking) telephone calls is permitted only with the consent of the subscriber or user. Any rejection of consent must be free of charge.

The Agency considers non-automated direct marketing by telephone to be a form of unsolicited communication under the ZEKom-1 and, therefore, imposes sanctions if the prior consent of the addressee has not been obtained.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Any direct marketing by telephone to corporate subscribers is permitted only with the prior consent of the addressee.

Exemptions and other issues

If an individual requests that the direct marketing calls cease, the person conducting the marketing activity is obliged to prevent the telephone number of the individual from being used for the purposes of direct marketing within 15 days upon having received such request, and should inform the addressee thereon within the following five days.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Utilisation of a personal fax number for the purpose of direct marketing is permitted only if the natural or legal person pursuing the marketing activity has obtained the prior consent of the individual addressee.

Conditions for direct marketing by fax to corporate subscribers

Direct marketing by fax to corporate subscribers is permitted only with the prior consent of the addressee.

Exemptions and other issues

No exemptions apply.

Spain.

General | Data Protection Laws

National Legislation

General data protection laws

The Organic Law 15/1999 relating to Personal Data Protection (*Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal)* (the "**DPA**") implemented the *Data Protection Directive*. The DPA has been further developed by Royal Decree 1720/2007 ("**Data Protection Regulations**").

Entry into force

The DPA entered into force on 14 January 2000, and Royal Decree 1720/2007 entered into force on 19 April 2008.

National Regulatory Authority

Details of the competent national regulatory authority

Agencia Española de Protección de Datos (the "**AEPD**")
Jorge Juan, 6
28001 Madrid, Spain
Tel +34 901 100 099

www.agpd.es

Notification or registration scheme and timing

Any person intending to create or modify personal data files is required to register with the AEPD by completing the forms (available on the AEPD website) prior to processing personal data. The notification of data files is free. The General Data Protection Register of the AEPD approves the notification if the notification form complies with the necessary requirements. It is a mere filing of information that must take place prior to the creation of the data file.

There is no charge for registration.

Exemptions

There are no exemptions from notification or registration.

Appointment of a data protection officer

A data protection officer is only required where medium or high security measures apply under the Data Protection Regulations (see "**Security**" below).

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. However, Data Protection Regulations have introduced the "business card" exception, i.e. data files that merely contain contact data for individuals working for legal entities are not subject to the DPA as long as the identities of the individuals are ancillary for the data processing. Additionally, the AEPD has held that opinions of one individual in respect of a second individual are not only the personal data of the second individual but also the personal data of the first individual providing the opinion.

Is information about legal entities personal data?

No. The DPA only applies to information about individuals as opposed to legal entities.

What are the rules for processing personal data?

The DPA includes most of the *standard conditions for processing personal data*. However, the legitimate interests condition (which permits processing solely on the basis that it is in the *data controller's* legitimate interests and does not prejudice the interests of the *data subject*) is only available in limited circumstances: (i) when the contractual exception to render a data processing legitimate applies; or (ii) when there is a national law that foresees such data processing. The European Court of Justice decided in 2011 that this is too restrictive and does not properly implement Article 7(f) of the *Data Protection Directive* (see *ASNEF and FECEMD v Administración del Estado*, C-468/10 and C-469/10). Nevertheless, so far there has not been any change in the DPA or in the interpretation of the DPA by the AEPD.

In practice, consent is frequently relied upon as grounds for processing non-sensitive personal data. Consent need not be in writing.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

There are no formalities under the DPA to obtain consent to process personal data, except in regard to sensitive personal data (see below). Consent can be express, written, oral or implied, however, it must be free, unambiguous, specific and informed. Furthermore, the *data controller* should keep adequate records to evidence the existence of such consent.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data means the *standard types of sensitive personal data*.

Are there additional rules for processing sensitive personal data?

Personal data revealing ideology, trade union membership, religion and beliefs may only be processed with the express, written consent of the *data subject*.

Personal data relating to racial origin, health or sex life may only be obtained, processed and disclosed when so provided by a law on grounds of general interest, or with the *data subject's* express consent. Data files containing sensitive data must implement high-level security measures (in addition to basic and medium-security measures they must, among other duties, encrypt the information when distributing it etc., as set out in the regulations on security measures).

The DPA only permits the processing of criminal records data where specifically provided for in law. In practice, only public entities with specific legal authorisation may hold data relating to criminal records.

Are there any formalities to obtain consent to process sensitive personal data?

Consent must be express and in writing.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

Data controllers and *data processors* are responsible for compliance and shall be subject to the sanctioning provisions of the DPA. In particular, the DPA applies to processing carried out by a *data processor* established in Spain (for example, the *data processor* will have to comply with the regulations on security measures).

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to data recorded on a physical medium that enables processing of the data, this includes both manual and electronic records.

Rights of Data Subjects

Compensation

Data subjects who, as a result of failure to comply with the provisions of the DPA on the part of the controller or processor, suffer damage to their possessions or rights shall have the right to damages. Nevertheless, damages for breach of the DPA are not commonly claimed nor awarded.

Fair processing information

Data subjects must be informed in advance expressly, precisely and unambiguously of the *fair processing information*. This includes: (i) the obligatory or voluntary nature of their reply to the questions put to them; (ii) the consequences of the collection of the data or of the refusal to supply the data; (iii) the possibility of exercising the rights of access, rectification, erasure and opposition. Furthermore, where questionnaires or other printed forms are used for the collection of personal data, they shall set out, in clearly legible form, the information referred to above.

The decisions of the AEPD show this can be an onerous obligation. In particular, it is not acceptable to use a broad description of the purposes for which the data is processed (such as use for "commercial purposes") and it may be necessary to list each individual recipient of the data (for example, references to the data being supplied to "members of the [X] group" may not be sufficient).

Additionally, when the consent of a *data subject* is sought by the *data controller* for purposes wider than the execution of a contract with the *data subject*, the *data subject* needs to be given the option of objecting to such additional data processing by easy means (for example, by ticking a box which is not pre-ticked).

There is no obligation in the DPA to provide this information in Spanish, though it may be difficult to show the information has been fairly provided if it is not in a language the *data subject* is familiar with. There is no obligation to refer to the DPA itself in any *fair processing information.*

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. The *data subject* shall be granted a free and simple means of exercising the right of access. The *data subject* is only entitled to exercise this right once per year, unless he justifies this by establishing that he has a legitimate interest to exercise his access right more often.

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing his personal data for direct marketing purposes. The *data controller* must then cease such processing within 10 days from receipt of the request.

Other rights

Data subjects have the right to object to the processing under specific circumstances.

Data subjects have the right to: (i) not be subject to a decision that produces legal effects based solely on automated processing of data; (ii) consult the General Data Protection Register; and (iii) compensation if they have suffered damage or injury to their property or rights as a result of the infringement of the DPA.

Security

Security requirements in order to protect personal data

Data Protection Regulations impose specific security obligations that must be used to protect personal data. The regulations classify the security measures into three levels: basic, medium and high, depending on the nature of the information processed, and make the distinction between automated data files and non-automated data files.

Specific rules governing processing by third party agents (processors)

The performance of processing operations by a *data processor* on behalf of a *data controller* must be governed by a contract stating the *standard processor obligations* permitting its conclusion and contents to be evidenced. The contract must expressly state that the *data processor* shall: (i) process the data only in accordance with the instructions of the *data controller*; (ii) not apply or use them for a purpose other than that set out in the said contract; and (iii) not communicate them to other persons even for their preservation.

The contract shall also oblige the *data processor* to comply with the security measures in the DPA and the Data Protection Regulations. Once the contractual service has been completed, the personal data must be destroyed or returned to the *data controller*, together with any support or documents containing personal data processed.

If the *data processor* uses the data for another purpose, communicates them or uses them in a way not in accordance with the terms of the contract, he shall also be considered as the *data controller*, and shall be personally responsible for the infringements committed by him. Sub-contracting by the *data processor* to a third party is only permitted if the contract between the *data controller* and the *data processor* contemplates such sub-contracting, identifying the processing to be sub-contracted and the identity of the sub-processor, and if the processing carried out by the sub-processor complies with the instructions of the *data controller*.

Notice of breach laws

The Data Protection Regulations do not contain any obligation to inform the AEPD or *data subject* of any breach. *Data controllers* in certain sectors may be required to inform sectorial regulators of any breach.

Specific notice of breach laws now apply to the electronic communications sector following the implementation into national law of the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the *standard conditions for transborder dataflow*, except that *transborder dataflows* subject to *Model Contracts* or *binding corporate rules* require prior authorisation from the Director of the AEPD. Spain is part of the mutual recognition club for *binding corporate rules*.

Notification and approval of national regulator (including notification of use of Model Contracts)

If the *standard conditions for transborder dataflow* are not met or *Model Contracts* are used, then international transfers are prohibited without prior authorisation from the Director of the AEPD.

Whether or not the transfer requires prior authorisation, it has to be notified to the AEPD. In this regard, the standard form to notify the creation of data files includes a section on international transfers. If this section is not completed when the file is initially notified, the notification must be amended to include the transfer.

Use of binding corporate rules

The Spanish regulator recognises the use of *binding corporate rules* in Spain. Nevertheless only a few transfers of data outside of the EEA have been approved based on *binding corporate rules*.

Enforcement

Sanctions

Spain has one of the most stringent penalty systems in the entire EU in the event of breach of the DPA, with fines of up to EUR 600,000 per infringement. The penalties established pursuant to the DPA range from EUR 900 to EUR 600,000, depending on the severity of the breach. Breach of the DPA implies fines but it must be noted that the Spanish Criminal Code also establishes a number of criminal offences derived from the violation of secrets and breach of privacy, although such criminal actions are not common.

Practice

In 2011, there were 5,294 investigations carried out by the AEPD, of which some were "preventative enforcement", rather than driven by a particular complaint lodged with the AEPD. There were 674 sanctioning proceedings resolved against private entities and 99 against public entities in that period. The total amount of fines imposed by the AEPD in 2011 was EUR 19,597,905.97. Frequently, the AEPD imposed the minimum level of fine for single infringements. Therefore, a standard fine imposed for a non-serious breach was EUR 900, for a serious breach EUR 40,001 and for a very serious breach EUR 300,001. Nevertheless, in some proceedings, the AEPD imposed a single fine that corresponds to several infringements, and in other cases, the AEPD imposed a fine for a higher amount than the minimum amount of the corresponding threshold.

The most relevant breaches of the DPA, penalised by the AEPD in 2011, relate to breaches or infringements carried out by telecommunications operators, CCTV, financial companies, internet services providers and unsolicited commercial communications sent by e-mail or fax.

Enforcement authority

The Spanish Enforcement Authority is the AEPD. It conducts investigations and brings disciplinary action relating to data protection issues. Its resolutions can be appealed before the courts, which in most cases confirm such resolutions. Proceedings for criminal offences are brought before the Spanish criminal courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Law 34/2002 on information society services and electronic commerce (the "**ECA**") implemented Article 13 of the *Privacy and Electronic Communications Directive*. The ECA is effective as of 12 October 2002.

The rest of the provisions concerning the processing of personal data and the protection of privacy in the electronic communications sector set out in the *Privacy and Electronic Communications Directive* such as itemised billing, traffic data, location data other than traffic data, directories of subscribers, etc. were incorporated into Spanish Law by Royal Decree 424/2005, which entered into force on 30 April 2005 as amended by Royal Decree 1768/2007.

The ECA has been amended to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

The ECA has been amended to implement the *Citizens' Rights Directive*. As a result of such amendment, it is necessary to inform users of the use of cookies and to obtain consent to the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user.

Regulatory guidance on the use of cookies

There is no regulatory guidance on the use of cookies.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

The ECA provides that it is forbidden to send advertising or promotional communications by e-mail, or by any other equivalent means, if they have not been requested or expressly authorised by the recipient of such communication.

Conditions for direct marketing by e-mail to corporate subscribers

The ECA provides that it is forbidden to send advertising or promotional communications by e-mail, or by any other equivalent means, if they have not been requested or expressly authorised by the recipient of such communication. The e-mail will include at the beginning of the message the word "advertising" or its abbreviation.

Exemptions and other issues

The *similar products and services exemption* applies. The ECA also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) an opt-out address is not provided.

The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Data processing for marketing purposes (including direct marketing by telephone to individual subscribers) carried out by human means is permitted if the requirements set down by the DPA are met. That is when: (i) the data are included in a source accessible to the public (including fixed telephony directories); or (ii) the prior informed consent has been obtained from the *data subject*.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

Direct marketing by telephone, which is addressed at an individual within a corporation must meet the requirements set out above for marketing by telephone to individual subscribers.

If the direct marketing by telephone carried out by human means is not aimed at individuals within a corporation but at a corporation itself, the DPA and the ECA apply no restrictions.

Exemptions and other issues

No exemptions apply.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Data processing for marketing purposes (including direct marketing by fax to individual subscribers) carried out by human means is permitted if the requirements set down by the DPA are met. That is when: (i) the data are included in a source accessible to the public (including fixed telephony directories); or (ii) the prior informed consent has been obtained from the *data subject*.

Conditions for direct marketing by fax to corporate subscribers

Data processing for marketing purposes (including direct marketing by fax to corporate subscribers) carried out by human means is permitted if the requirements set down by the DPA are met. That is when: (i) the data are included in a source accessible to the public (including fixed telephony directories); or (ii) the prior informed consent has been obtained from the *data subject*.

If the direct marketing by fax by human means is not aimed at individuals within a corporation, but at a corporation itself, the DPA and the ECA apply no restrictions.

Exemptions and other issues

No exemptions apply.

Sweden.

General I Data Protection Laws

National Legislation

General data protection laws

The Swedish Personal Data Act (Sw. *Personuppgiftslagen* (1998:204)) (the "**Act**") implemented the *Data Protection Directive*.

Entry into force

The Act entered into force on 24 October 1998 but due to transitional regulations it only entered into full force on 1 October 2001. The Unstructured Material Rule (see below) entered into force on 1 January 2007.

National Regulatory Authority

Details of the competent national regulatory authority

Datainspektionen (the "**Data Inspection Board**")
Box 8114
SE-104 20 Stockholm
Sweden

www.datainspektionen.se

Notification or registration scheme and timing

There is a general duty to notify the Data Inspection Board about the processing of personal data. This merely requires a filing of information and does not require any approval. The notification must occur prior to the first processing of personal data. There is no charge for notification.

Exemptions

The notification duty only includes processing of data that is completely or partially automated. In addition, there are several exceptions to the general notification duty. The notification duty does not apply, for example, if the *data subject* has given his/her consent to the processing or if the *data controller* has appointed and registered a personal data representative. Neither is notification required if the personal data processed is non-sensitive and relates to a *data subject* with whom the *data controller* has a certain relationship (such as follows from employment, membership, customer relationship or similar) if the *data controller* maintains a schedule of the processing including such information as would otherwise have been included in a notification. In addition, notification is not required when processing personal data in accordance with the Unstructured Material Rule (see below).

Appointment of a data protection officer

There is no legal obligation to appoint a personal data representative. However, the appointment and registration with the Data Inspection Board of such a person exempts the *data controller* from the obligation to notify (see above).

Personal Data

What is personal data?

The definition of personal data in the Act is closely based on the *standard definition of personal data*. In particular, it only applies to living individuals, as opposed to deceased persons. The Swedish courts and regulator tend to interpret the concept of personal data broadly. The guidelines issued by the regulator are, however, in all relevant respects in line with the *Opinion on Personal Data*.

IP addresses are considered as personal data. This has been confirmed by the Administrative Court of Appeal, which has stated that an IP address is referable to a natural person and shall therefore be considered as personal data.

Is information about legal entities personal data?

No. The Act only applies to information about living individuals. However, information on sole traders is considered personal data as such private businesses consist of an individual.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the legitimate interests condition is frequently relied upon as grounds for processing non-sensitive personal data.

Are there any formalities to obtain consent to process personal data?

Consent must be a voluntary, specific and unambiguous expression of will. It does not have to be made in writing. Implied consent would, according to the Data Inspection Board, be sufficient only if the personal data is not sensitive. However, regardless of whether the data is sensitive or not, tacit, silent or hypothetical consent is not sufficient. As consent must

be given voluntarily, it is not advisable to rely solely on consent in relation to employees, since the employee must be able to refuse to consent and may also withdraw his/her consent at any time.

Sensitive Personal Data

What is sensitive personal data?

Under the Act, sensitive personal data includes the *standard types of sensitive personal data*.

Certain alternative provisions apply to information about legal offences and personal identity numbers (the Swedish equivalent of social security numbers).

Are there additional rules for processing sensitive personal data?

In general, sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met.

Data concerning legal offences may, subject to a few exemptions, only be processed by public authorities unless permission is granted by the Data Inspection Board.

Personal identity numbers may, in the absence of consent, only be processed when it is clearly justified with regard to the purpose of the processing, the importance of secure identification or some other noteworthy reason.

None of the restrictions described above need to be observed when processing personal data in accordance with the Unstructured Material Rule.

Are there any formalities to obtain consent to process sensitive personal data?

A *data subject's* consent does not have to be made in writing but must be voluntary, explicit and informed.

Scope of Application

What is the territorial scope of application?

The Act applies the *standard territorial test*. The Data Inspection Board has indicated that the criteria "established" shall be interpreted extensively.

Who is subject to data protection legislation?

The *data controller* is responsible for compliance with the Act. *Data processors* are not subject to the Act.

Are both manual and electronic records subject to data protection legislation?

Yes. The Act applies to processing of personal data that is: (i) wholly or partly automated (i.e. an electronic register that is connected to data stored manually); and (ii) otherwise processed (i.e. not automated), if such personal data is included in a structured collection of data available to be searched according to certain criteria.

Furthermore, in relation to automated processing, the great majority of the provisions of the Act need not be applied when processing personal data in unstructured material, i.e. personal data that does not form part, and is not intended to form part, of a set of personal data that has been structured in order to significantly facilitate searches for, or compilations of, personal data. In short, the basic rule of the Act with regard to processing of personal data in unstructured material (such as e-mails, word processing documents, sounds and images) is that such processing is permitted, provided that the processing does not lead to infringement of the *data subject's* privacy (the "**Unstructured Material Rule**").

Rights of Data Subjects

Compensation

Data subjects have a right to compensation for any damage or violation of personal integrity caused by the processing of personal data in contravention of the Act.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. The *data controller* must also provide all other information necessary in order for the *data subject* to be able to exercise his/her rights in connection with the processing. Such information shall include, *inter alia*, information about the recipients of the personal data, the obligation to inform and the *data subject's* rights. The Data Inspection Board has stated that it cannot be expected that the *data subject* understands languages other than Swedish, hence the information should be provided in Swedish unless, for example in relation to employees, the *data subjects* are required, as part of their employment, to be fluent in another language. There is no obligation to refer to the Act in the *fair processing information*.

If personal data has been obtained from a third party rather than the *data subject*, the *fair processing information* need not be provided if it is impossible or if it would involve a disproportionate effort.

A *data controller* is not required to provide information to *data subjects* when processing personal data in accordance with the Unstructured Material Rule.

Rights to access information

Every *data subject* is, once a year and free of charge, entitled, upon written request, to receive their *subject access information* by written request to *data controllers*. The rights of access need not be observed when processing personal data in accordance with the Unstructured Material Rule.

Objection to direct marketing

Personal data may not be processed for purposes of direct marketing if the *data subject* notifies the *data controller* in writing that he/she opposes such processing. The *data controller* must cease such processing when the notification reaches the *data controller*.

Other rights

The *data subject* is entitled to obtain immediate rectification, blocking or erasure of any personal data that has not been legally processed under the Act.

The rights of correction need not be observed when processing personal data in accordance with the Unstructured Material Rule and, in such situations, the *data subject* has no right to object to such processing.

Security

Security requirements in order to protect personal data

The *data controller* must comply with the *general data security obligations*. This also applies when processing personal data in accordance with the Unstructured Material Rule.

Specific rules governing processing by third party agents (processors)

If the *data controller* engages a *data processor*, the parties must enter into a written contract. The contract must stipulate that the *data processor* complies with the *standard processor obligations*. This also applies when processing personal data in accordance with the Unstructured Material Rule.

Notice of breach laws

The Act contains a general obligation for the personal data representative to inform the Data Protection Board of any suspected breaches of the Act.

Specific notice of breach laws applies to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transfer of personal data to third countries (i.e. countries outside the EU/EEA) is prohibited unless the third country has an adequate level of protection or the *standard conditions for transborder dataflow* are satisfied. The *data controller* can make its own assessment of whether the personal data will be adequately protected after it has been transferred to a third country.

The transfer prohibition need not be observed when processing personal data in accordance with the Unstructured Material Rule.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no obligation to notify or obtain the consent of the Data Inspection Board to any *transborder dataflows*. However, the Data Inspection Board has stated that, to the extent a *data controller* wishes to claim that there is other adequate protection (such as the use of *binding corporate rules*) for the transfer of the personal data, the *data controller* must apply to the Data Inspection Board for an exemption from the prohibition to transfer personal data to a third country. There is no obligation to notify the Data Inspection Board or obtain its consent to use the *Model Contracts*.

Use of binding corporate rules

The use of *binding corporate rules* is recognised in Sweden. However, the Data Inspection Board has not signed up to the mutual recognition process and, consequently, a separate application to the Data Inspection Board is required.

Enforcement

Sanctions

Certain violations of the Act may lead to fines or imprisonment for a maximum of six months or, if the crime is major, to imprisonment for a maximum of two years. A sentence is not imposed in minor offences.

Practice

According to the Data Inspection Board's annual report for 2011, the Data Inspection Board initiated 247 inspection matters in total during 2011, which is an increase compared to previous years.

The typical penalties imposed for violations of the Act are fines and damages, awarded to the victim. The level of the penalty varies according to the severity of the crime and the income of the person responsible for the breach of the data protection legislation.

There have been cases of imprisonment for breaches of the data protection legislation, in particular cases where the infringer has committed other additional offences, for example, severe defamation. Another case which involved imprisonment for breach of the data protection legislation concerned two persons with Nazi leanings who set up a register containing details of religious and political beliefs, sexual life and race for a large group of people. The sentence referred mainly to the breach of the data protection legislation. One of the victims of the infringement received SEK 10,000 in damages (approximately EUR 1,070 at the time).

Enforcement authority

The Data Inspection Board has the authority to fine organisations and prohibit organisations from processing personal data. The decisions of the Data Inspection Board can be appealed to the Swedish Administrative Courts. The Data Inspection Board may also apply to the Swedish Administrative Courts to delete unlawfully processed personal data.

Prosecutions for criminal offences are brought before the Swedish General Courts by the Public Prosecutors and may lead to fines or imprisonment. Claims for damages awarded to compensate the *data subject* for violation of personal integrity are also brought before the Swedish General Courts, often integrated with the criminal proceedings.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

A modification of the Marketing Act (Sw. *marknadsföringslagen* (1995:450)) on 1 April 2004 implemented Article 13 of the *Privacy and Electronic Communications Directive*. A new Marketing Act (2008:486) entered into force 1 July 2009.

The Electronic Communications Act (Sw. lagen om elektronisk kommunikation (2003:389)) was amended on 1 July 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user that the subscriber or user explicitly has requested.

Regulatory guidance on the use of cookies

The Swedish Post and Telecoms Authority (*Sw. post- och telestyrelsen*; "**PTS**") is the national regulatory authority that monitors the electronic communications and postal sectors in Sweden. PTS has issued general guidance on the use of cookies, which can be found on the authority's web site. However, considering the recent implementation of the requirement of consent to the use of cookies, PTS has not issued any guidance on how consent shall be obtained for a certain website except that consent shall be a conscious approval. Instead, PTS, has explicitly stated that it considers the website holders to be best positioned to work out functional and secure solutions for how consent shall be obtained and that PTS would like to give the web site holders time and space to find solutions that work for both the website and the users.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Direct marketing by e-mail is in principle only permitted if the recipient has given his/her consent.

Conditions for direct marketing by e-mail to corporate subscribers

The restrictions do not apply to corporate subscribers.

Exemptions and other issues

Direct marketing by e-mail does not require consent if the *similar products and services exemption* applies. In such case, a valid opt-out address must always be provided. The sender must also include the *eCommerce information* and other information that could be of particular importance from a consumer's perspective, if any.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Direct marketing by telephone is permitted unless the individual has clearly opposed such marketing.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The rules on direct marketing by telephone are not applicable in relation to corporate subscribers.

Exemptions and other issues

No exemptions apply.

The recipient must be told who is responsible for the marketing and must be provided with information that could be of particular importance from a consumer's perspective.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Direct marketing by fax is only permitted if the recipient has given his/her consent.

Conditions for direct marketing by fax to corporate subscribers

The rules on direct marketing by fax are not applicable in relation to corporate subscribers.

Exemptions and other issues

No exemptions apply. The recipient must be told who is responsible for the marketing and must be provided with information that could be of particular importance from a consumer's perspective.

Switzerland.

Contributed by Homburger AG

General | Data Protection Laws

National Legislation

General data protection laws

The Swiss Federal Data Protection Act (the "**DPA**") is dated 19 June 1992. The DPA follows similar concepts as the *Data Protection Directive*. Accordingly, the European Commission has found Switzerland to provide an adequate level of data protection from an EU perspective (Decision 2000/518/EC).

Entry into force

The DPA came into force on 1 July 1993; a revised version has been in force since 1 January 2008, with some minor revisions since. A revision is currently being discussed again, but several years away.

National Regulatory Authority

Details of the competent national regulatory authority

The Swiss Federal Data Protection and Information Commissioner (the "**DPIC**")
Feldeggweg 1
CH-3003 Berne
Switzerland

www.edoeb.admin.ch

Notification or registration scheme and timing

Data controllers which regularly process sensitive personal data or personality profiles or regularly disclose personal data to third parties must register their data collection with the DPIC. This registration does not require any approval and is, therefore, a mere notification system. The registration must take place before the data collection is established. There are no registration fees. The register is publicly accessible over the internet. At the end of 2012, 914 data collections had been registered by the private sector.

Exemptions

No registration is required if: (i) the data are processed due to a statutory obligation of Swiss law; (ii) a data protection officer has been appointed who independently monitors internal compliance with data protection regulations and maintains a list of the data collections, and such data protection officer has been notified to the DPIC (and meets the requirements of the DPA); (iii) the *data controller* has acquired a data protection quality mark (regarding the data collection in issue) under a certification procedure in accordance with the DPA and has notified the DPIC of the result of the evaluation; (iv) the data are used exclusively for publication in the edited section of a periodically published medium and are not passed on to third parties without informing the *data subjects*; (v) the data are processed by journalists who use the data file exclusively as a personal work aid; or (vi) one of the further exemptions provided for in the Ordinance to the DPA applies (for example, for publicly accessible data collections, for client and supplier files (provided they do not contain any sensitive personal data or personality profiles) and for bookkeeping records).

Appointment of a data protection officer

There is no legal requirement to appoint a data protection officer. However, doing so can exempt a *data controller* from the requirement to register (see above). By the end of 2012, 699 companies in the private sector have appointed a data protection officer and notified the appointment to the DPIC (in order to be exempted).

Personal Data

What is personal data?

The definition of personal data in the DPA is closely based on the *standard definition of personal data*. The term is understood rather broadly. Nevertheless, the *Opinion on Personal Data* has not been fully and formally adopted in Switzerland (for instance, the fact that a particular set of data could some time in the future affect a particular individual is not sufficient for such data to be considered personal data). Also, website usage data collected by a site operator using "cookies" are not considered personal data as long as the *data subject* is not and cannot be reasonably identified by the operator.

However, IP addresses may qualify as personal data, as recently confirmed by the Federal Supreme Court (DFC 136 II 508, *Logistep*). While this may not be the case in all circumstances, if IP addresses are collected for the very purpose of identifying the individuals behind them (such as people illegally sharing pirated content over the internet), and if Swiss law permits such identification (which it does in the case of internet felonies), then IP addresses should be treated as personal data (it should be noted that the court found that in the case at hand it was not permissible under the DPA to

collect such personal data for the purpose of identifying individuals illegally sharing pirated content, although the balancing of interests in this case has been heavily criticized). Swiss law thus follows a "relative" definition of personal data: for data to be considered personal data, the relevant audience must not only be able to identify the *data subjects*, but also willing to undertake such efforts. Accordingly, if personal data is securely encrypted, it no longer is considered personal data for those who are not able to decrypt it.

Is information about legal entities personal data?

Yes. The DPA extends to include information not only about individuals, but also about legal entities (this is interpreted broadly to include partnerships and trusts). The processing of personal data of legal entities is subject to the same provisions as the processing of personal data of individuals.

What are the rules for processing personal data?

Personal data may be processed if the processing either: (i) does not violate the personality of the *data subject*; or (ii) does violate the personality of the *data subject*, but is justified by the *data subject's* consent, an overriding private or public interest or by a provision of Swiss law requiring or permitting the processing at issue. Any legitimate interest of the *data controller*, the *data processor*, the *data subject* or any third party can, in principle, qualify as an overriding private interest if it is sufficient to outweigh the violation of the *data subject's* personality. However, the Federal Supreme Court recently held that *data controllers* should be cautious before assuming that private interests will justify any such processing (DFC 136 II 508). In another case involving the online service "Street View" (the "**Street View Case**"), however, the Federal Supreme Court found that the public interest justifies keeping the service alive although the algorithm for blurring faces was not perfect and missed 1 percent of the visible faces (DFC 138 II 346). The DPA provides a non-exhaustive list of circumstances in which the overriding private interest of the *data controller* must be considered, for example: (i) the conclusion and performance of a contract with the *data subject*; (ii) the processing of information on competitors; or (iii) the processing of personal data for non-personal uses.

The personality of the *data subject* is, by definition, considered violated if its personal data: (i) are not processed lawfully (for example, if data have been stolen or extorted from someone else); (ii) are not processed in good faith; (iii) are processed for purposes neither indicated at the time of collection, nor evident from the circumstances, nor provided for by (Swiss) law; (iv) are not processed in a proportionate manner (are not or are no longer necessary or suitable in view of the purpose of processing, or are for an excessive purpose); (v) have been collected without such collection and in particular the purpose of their processing being made, depending on the circumstances, noticeable or evident to the *data subject* (even if such processing is provided for by law); (vi) have not been verified for their correctness (where necessary); (vii) are being processed without complying with the *general data security obligations*; (viii) are processed against the *data subject's* express will; (ix) are sensitive personal data or personality profiles and are disclosed to a third party (see below); or (x) are employee personal data and are processed despite being neither necessary for assessing the qualification of the employee for his/her job nor for the performance of his/her employment contract.

Notwithstanding the foregoing, it is presumed that the personality of the *data subject* is not violated if the *data subject* has made the data generally accessible and has not expressly prohibited their processing. However, the *data subject* can challenge this and prove that its personality has nevertheless been infringed upon, for example by the abusive use of information published on the *data subject's* website.

Although the DPA follows a slightly different approach with regard to the rules for the processing of personal data than the *Data Protection Directive*, the processing of personal data is in practice usually permissible if the *standard conditions for processing personal data* are met.

Are there any formalities to obtain consent to process personal data?

Consent is valid only if given voluntarily following the provision of adequate information ("informed consent"). Furthermore, consent is only effective if given in advance of processing. Consent need not be given in writing; however, the burden of proof is upon the *data controller* or *data processor*, respectively, so this would be recommended for evidentiary purposes. Implicit consent may be sufficient, in certain circumstances, but not in regards to sensitive personal data or personality profiles (see below).

The failure of a *data subject* to object to a particular processing or notice of such processing of his/her personal data is usually not sufficient to presume consent.

A *data subject* may withdraw his/her consent at any time, although such withdrawal will not usually be applied retrospectively. Even if a *data subject* has withdrawn his/her consent, depending on the circumstances, it may still be possible to justify a particular processing of personal data under the argument of an overriding private interest of the *data controller*, the *data subject* or other party.

Employees can, in principle, validly consent to the use of their personal data by the employer. However, if such consent is provided for in an agreement (for example, the employment contract), it shall be considered null and void if: (i) the employee is asked to consent to the processing of personal data which is neither required for assessing the qualification of the employee for his/her job nor for the performance of his/her employment contract; and (ii) the processing of such data is, from an overall perspective, to the employee's detriment. It may also be hard to demonstrate that the consent of an employee has been given voluntarily.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data include: (i) the *standard types of sensitive personal data* (except for data related to ethnic origin, which do not form part of the definition under the DPA, and health data, which only cover personal data such as a handicap or illness of the *data subject*); (ii) personal data on religious, ideological or political activities (not only related beliefs); (iii) the intimate sphere as such (not only sex life); (iv) social security measures; and (v) administrative or criminal proceedings and sanctions.

Biometric data do not uniformly qualify as sensitive personal data and must be assessed as to whether they fall under one of the categories defined above. The question of whether a photograph of a *data subject* qualifies as sensitive personal data (as it reveals the racial origin of the *data subject*) has not yet been decided under Swiss law; however, there has not been much support in favour of such a broad interpretation of the term.

It should be noted that, under the DPA, the rules for sensitive data also apply to personality profiles. These are combinations of data that allow the assessment of fundamental characteristics of the personality of an individual (for instance, the personnel file of an employee or data on the purchasing pattern of a credit card holder will, in practice, often amount to a personality profile).

Are there additional rules for processing sensitive personal data?

Sensitive personal data (and personality profiles) may not be disclosed to third parties without sufficient justification such as: (i) the *data subject's* consent; (ii) any overriding private or public interest; or (iii) a provision of Swiss law requiring or permitting such disclosure. If one of the *standard conditions for processing sensitive personal data* is met, this is usually a sufficient justification.

Furthermore, if sensitive personal data or personality profiles are (systematically) collected for a data collection, the *data subject* has to be expressly informed about the collection of such data, and regular processing of such data may require a registration with the DPIC (see the section "Notification or registration scheme and timing" above).

Are there any formalities to obtain consent to process sensitive personal data?

In the case of sensitive personal data (or personality profiles), the *data subject's* consent may be relied upon only if it has been given explicitly. However, consent need not be given in writing; but, as with non-sensitive personal data, this is recommended (see above).

Scope of Application

What is the territorial scope of application?

The DPA's registration and notification obligations apply to data collections being processed in and exported from Switzerland, respectively.

In the case of civil lawsuits against a person participating in a violation of personality, Swiss courts will in general apply the DPA, upon free choice of the *data subject*, if either: (i) the *data subject* is resident in Switzerland (provided this was foreseeable for the *data controller* or *data processor* sued); (ii) the *data controller* or *data processor* sued has its seat of residence or a branch in Switzerland; or (iii) the place of effect of the violation of personality (which usually includes the place of processing of personal data) is in Switzerland (provided this was foreseeable for the *data controller* or *data processor* sued). In the Street View Case, the Federal Supreme Court confirmed the applicability of Swiss data protection law, despite the service being provided from outside of Switzerland (DFC 138 II 346).

Who subject to data protection legislation?

Everyone who processes personal data must comply with the DPA. Accordingly, not only *data controllers* but also *data processors* are responsible for compliance. Hence, the obligations of *data processors* may go, at least in theory, beyond the *standard processor obligations*. In fact, even persons who are neither *data controllers* nor *data processors*, but otherwise "participate" in the processing of personal data may be held responsible in case of a civil claim.

Cantonal and local authorities are governed by separate, cantonal data protection legislation, not the DPA (however, certain provisions of the DPA apply if the cantonal data protection legislation fails to provide for adequate protection). Federal authorities (including private persons entrusted with public tasks, such as those in the field of mandatory health insurance) are also subject to the DPA, but: (i) must comply with additional rules (for example, the processing of personal data is normally permitted only on the basis that there is a provision of Swiss law that permits such processing); and (ii) cannot rely on the same reasons for justifying a violation of a *data subject's* personality as private persons can do.

The DPA does not apply to personal data processed by an individual solely for personal purposes and not disclosed to third parties. Another important exception is that the DPA does not apply to pending civil, criminal, international judicial assistance and administrative recourse proceedings in Switzerland.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies irrespective of the technology used. However, the *general data security obligations* may have to be implemented differently depending on whether manual or electronic records are used. In the case of automated processing of personal data, additional security and documentation requirements apply (for example, the obligation to implement audit trails, where they are necessary to ensure the data protection of sensitive personal data and personality profiles).

Rights of Data Subjects

Compensation

Data subjects may claim for damages, satisfaction and/or surrender of profits if their personality has been violated without sufficient justification. Damages and/or satisfaction may only be claimed in cases of negligence or wilful intent. The prerequisites for claims for surrender of profits are not entirely clear for violations of personality (one may assume, though, that a claim will be possible only in the case of bad-faith behaviour). So far, there have been hardly any civil lawsuits on the basis of the DPA. Most cases that involve the protection of a *data subject's* personality are mass-media-related, employee-related and insurance surveillance cases.

Fair processing information

The collection of personal data and in particular the purpose of their processing has to be, depending on the circumstances, noticeable or evident to the *data subject*, unless there is a sufficient justification not to comply with this requirement (such as the *data subject's* consent, an overriding private or public interest or a provision of Swiss law).

Notwithstanding this, the *data controller* has to expressly inform *data subjects* about any (systematic) collection of sensitive personal data or personality profiles for a data collection. The information has to identify the *data controller*, the purpose of the processing of the data and the categories of recipients (in case it is planned to disclose such data). This obligation to inform also applies when such data are obtained through/from a third party, provided the *data subjects* have not yet been informed. Only a few exceptions apply. The *data controller* may, for instance, limit, defer or deny the information in the case of an overriding self-interest, provided, however, that the data will not be shared with third parties (which term also includes group companies).

There is no requirement for fair processing notices to be in one or all of the official languages of Switzerland, but the notice has to be in a language that the *data subjects* can understand, to be effective. Hence, on an English language website, the "privacy policy" has to be in English, and on a website also targeting a German-speaking audience, the notice also has to be in German.

Rights to access information

Data subjects may request from *data controllers* (and in specific cases also the *data processor*): (i) confirmation as to whether they process personal data relating to them; (ii) information as to all personal data relating to them that are contained in the *data controller's* data collection (including any available information on the source of the data); (iii) the purposes of the processing and, where applicable, the legal basis for the processing; (iv) the categories of personal data concerned; (v) the persons involved in the processing of the data collection; and (vi) the recipients to whom the data are disclosed.

Access may only be limited, deferred or denied under limited circumstances defined by the DPA, such as overriding third party interests, professional secrecy and other statutory obligations and, in limited circumstances, own overriding private interests. While it is, in principle, possible that an access request can be denied also on the basis of abuse of law, the Federal Supreme Court has set the bar relatively high for such denials. A client of a Swiss bank tried to use an access request to obtain a copy of internal client notes of the bank to evaluate the chances of a civil liability claim. The court did not consider this an abusive request; as it was not made solely for the purposes of a fishing expedition, but also for allowing the *data subject* to verify whether the personal data on record was correct (DFC 138 III 425).

Requests are usually to be made and responded to in writing, but, under certain conditions, electronic requests and responses are also admissible, as may be other forms (such as on-site reviews). Requests are usually free of charge and the *data subjects* making such requests must identify themselves (for example, by providing a photocopy of an ID).

Objection to direct marketing

The DPA provides for a general right of a *data subject* to object against the further processing of its personal data, but does not specifically address the issue of direct marketing.

Other rights

The *data subject* may request the personal data to be rectified, marked as being disputed or deleted. The *data subject* may request that no personal data be disclosed to third parties or processed further. The DPA does not include any specific provision with regard to decisions being taken based solely on automatic processing of personal data.

In addition to the requests for compensation described above, if necessary, a *data subject* can request a (civil) court to issue: (i) a restraining order (on a permanent or temporary basis); or (ii) declaratory relief or another appropriate order against a *data controller* or *data processor* to prevent or remedy an illegal violation of a *data subject's* personality.

Security

Security requirements in order to protect personal data

Data controllers and *data processors* must comply with the *general data security obligations*.

Specific rules governing processing by third party agents (processors)

Processing of personal data may be outsourced to a third party: (i) if the *data controller* ensures that the data are only processed in the way that the *data controller* would be entitled to; and (ii) if no statutory or contractual confidentiality obligations prohibit the outsourcing. The *data controller* must ensure that the third party complies with the *general data security obligations*. To the extent that certain data processing requires a particular justification, the third party may rely on the same justifications as the *data controller*. In practice, these rules usually require the *data controller* to enter into a contract with the *data processor* in order to ensure the *standard processor obligations* are complied with.

Notice of breach laws

The DPA does not contain any notification obligation in case of data breaches. However, the basic requirement to process personal data in good faith may require notices to be given to *data subjects* or third parties (such as a credit card company in the case of a loss of credit card information) or that other steps be taken. It is not necessary to inform the DPIC; however, in cases of serious breaches (especially breaches involving a large number of *data subjects* or that may cause media attention), it may be advisable to inform the DPIC.

Moreover, *data controllers* in certain sectors may be required to inform sector regulators of relevant breaches (for example, financial service providers may be required to inform the Swiss Market Supervisory Authority). Public companies may in very rare cases be required to make ad-hoc disclosures under the applicable listing rules.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

In principle, personal data may only be transferred to countries with legislation providing for an adequate level of protection of personal data. According to a (non-binding and non-concluding) list of countries with adequate data protection published by the DPIC, the EU Member States that have implemented the *Data Protection Directive* are, among others, considered to provide an adequate level of data protection (with regard to personal data related to individuals), as well as the *whitelisted countries* and the U.S. for those companies or organisations who have self-certified themselves under the U.S.-Swiss "Safe Harbor" framework (which mirrors the EU-U.S. "Safe Harbor" framework).

If data are to be transferred to a foreign country that does not have legislation providing an adequate level of data protection, one of the following conditions must be fulfilled: (i) the existence of a transborder dataflow contract or other "sufficient safeguards" to ensure an adequate level of data protection abroad; (ii) sufficient *binding corporate rules* concerning data protection in case data are transferred within a company or a group of companies (however, there is no need to have such rules approved by the DPIC); (iii) the *data subject's* consent to the data export in the specific case at issue; (iv) the export of the personal data at issue is required for the conclusion or performance of a contract with the *data subject*; (v) the export of the personal data is, in the specific case at issue, necessary for maintaining overriding public interests or establishing, exercising or enforcing legal claims or rights in court proceedings; (vi) the export of the personal data is, in the specific case at issue, necessary to protect the life or physical integrity of the *data subject*; or (vii) the *data subject* itself has made the personal data publicly available and not expressly prohibited the processing of such data. Therefore, the *standard conditions for transborder dataflow* generally also apply under the DPA, but with some deviations (such as the absence of a requirement to use *Model Contracts* in cases in which an exporter relies on contractual safeguards).

The DPIC offers a simple (controller-processor) model contract on its website specifically designed for Swiss law; however, the more complicated *Model Contracts* are also considered acceptable in most respects. The EU-U.S. "Safe Harbor" framework is not specifically recognised by the DPA, but is likewise considered as a "sufficient safeguard" for ensuring an adequate level of data protection in the case of personal data transfers to the U.S., provided, however, that the data importer commits itself to extend and apply its existing EU-U.S. "Safe Harbor" policy to also cover personal data from Switzerland (this way, the "Safe Harbor" self-certification process does not have to be formally repeated for Switzerland, as described above).

Accordingly, as a rule of thumb, data exports undertaken in compliance with the *standard conditions for transborder dataflow* are usually and generally speaking also in compliance with the DPA.

Notification and approval of national regulator (including notification of use of Model Contracts)

Data controllers have to notify the DPIC if they rely on transborder dataflow contracts, on *binding corporate rules*, or on other safeguards for ensuring an adequate level of data protection abroad for data collections being exported. There is no

obligation to obtain any approval from the DPIC. However, the DPIC will usually comment, within 30 days, on whether it considers the safeguard notified to be a sufficient safeguard.

A simplified notification procedure applies if *data controllers* are using a safeguard which has been officially recognised by the DPIC (so far, the official Swiss model contract, the *Model Contracts*, the Council of Europe model contract and the EU-U.S. "Safe Harbor" framework). It should be noted that no notification is required if an export to the U.S. is based on the U.S.-Swiss "Safe Harbor" framework.

From January 2008 (when the aforementioned duty to notify was first introduced in the DPA) to the end of 2012, 462 notifications were made to the DPIC.

Use of binding corporate rules

The use of *binding corporate rules* is generally recognised by the DPA as a method for achieving an adequate level of data protection abroad. There are no specific formal requirements. No DPIC approval is required or possible (however, as mentioned in the foregoing section, the *binding corporate rules* have to be notified to the DPIC).

Enforcement

Sanctions

The *data subject* is entitled to civil remedies such as damages and legal redress. A breach of privacy is not of itself a criminal offence.

In addition, individuals who are in breach of their obligations of information (in the case of the collection of sensitive personal data or personality profiles for a data collection), subject access right, registration, notification and co-operation with the DPIC may be fined up to CHF 10,000. More severe criminal sanctions may apply for breaches of professional secrecy. However, in practice, there are hardly any cases in which criminal sanctions have been imposed on *data controllers*.

Practice

There are no official statistics on the number of investigations and prosecutions concerning violations of the DPA. Between April 2011 and March 2012, the DPIC conducted 11 official investigations concerning the processing of personal data in the private sector; however, 6 of them resulted in a "recommendation" (see the section entitled "**Enforcement authority**" below), and one was submitted to the Federal Administration Court (which can be done if a recommendation is either not accepted or not complied with). The number of DPA-related cases decided by civil or criminal courts is not known. It is known, however, that since coming into force in 1993 and as of December 2009, the criminal provisions of the DPA have resulted in only one conviction (a five-day term plus a fine of CHF 750 in 1996).

In addition to the criminal provisions of the DPA, the Swiss Penal Code provides that a person who obtains sensitive data or personality profiles from a non-public data collection without authorisation shall be punished by imprisonment or fined. Since 1993 and as of December 2011, the foregoing provision has led to a total of 12 recorded criminal convictions (on average 0.6 per year).

Enforcement authority

The DPIC has no power to impose civil and/or criminal sanctions (including fines) in the private sector. However, the DPIC may conduct investigations in the private sector if a particular method of data processing could violate the privacy of a larger number of people (in addition to supervising the federal authorities' DPA compliance). Based on such investigations in the private sector, the DPIC may issue case-specific "recommendations" and may publish them. The recommendations themselves are not binding; however, if they are not complied with or are rejected, the DPIC may ask the Federal Administration Court to review them and, where appropriate, require the addressee to comply with them (by means of a binding court order); further recourse is possible to the Federal Supreme Court. Also, the DPIC is entitled (but not obliged) to notify the prosecuting authorities of suspected violations of the criminal provisions of the DPA (see the section entitled "**Sanctions**" above).

Further, upon an appropriate and justified request by a *data subject* or by the DPIC, the Swiss civil courts or the Federal Administrative Court, respectively, may: (i) issue temporary restraining orders against *data controllers* and/or *data processors*; (ii) stop a particular processing of personal data; or (iii) impose other measures the court considers appropriate to remedy or prevent a particular unjustified violation of personality of a *data subject*. The DPIC successfully made use of this power for the first time in December 2008 (Federal Administrative Court Decision of 14.01.2009, A-8028/2008, *Dun & Bradstreet*).

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Switzerland has implemented a provision that is similar to Article 13 of the *Privacy and Electronic Communications Directive*. The provision is part of the Swiss Unfair Competition Act and has been in effect since 1 April 2007.

Also, since 1 April 2012, the Swiss Unfair Competition Act has introduced a kind of an official Swiss "Robinson List" requiring businesses to comply with generic opt-out marks in the telephone directory for the purposes of commercial communications and the disclosure of data for the purposes of direct marketing. The term "telephone directory" refers only to the official directories of subscribers maintained by the registered telecom service providers in Switzerland pursuant to the Telecommunications Act. The opt-out marks currently apply to individual phone numbers and e-mail-addresses, not the entire address or record. The provision does not prevent direct marketing to current or recent customers and to people who have requested or consented to receiving the marketing materials.

Finally, the Telecommunications Act contains a provision on cookies roughly in line with Article 5(3) of the (original) *Privacy and Electronic Communications Directive* The violation of the provision can result in civil claims and, upon the request of a person affected, in criminal charges.

Cookies

Conditions for use of cookies

Cookies that do not contain or relate to personal data (i.e. that are not connected to persons identified or identifiable from the perspective of the person using the cookies) are not restricted (e.g., typical session cookies). If cookies (or similar techniques such as clear GIFs or web-beacons) are related to identified or identifiable persons or otherwise connected to personal data, then they may be used only if: (i) the they are required for the provision of telecommunications services or invoicing of such services; or (ii) the user has been informed about their processing, their purpose and that the user can decline the processing of related data. However, there is so far no requirement under Swiss law to obtain the user's consent for using cookies.

Regulatory guidance on the use of cookies

No.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Pursuant to the Swiss Unfair Competition Act, sending unsolicited mass direct marketing e-mails is only allowed if the recipient has provided his prior consent. The recipient's consent does not necessarily have to be in writing. However, it is not permissible to obtain consent by sending out unsolicited mass e-mails asking for such consent.

Since 1 April 2012, a new provision in the Swiss Unfair Competition Act requires businesses performing direct marketing to consult the official Swiss phone directories for e-mail-addresses that have been marked with a standardized telemarketing opt-out declaration, unless the person has otherwise consented in receiving e-mail marketing or has a customer relationship.

Furthermore, according to case law under the DPA, e-mail marketing is admissible only with the prior express consent of the intended recipients. It has been ruled that sending unsolicited e-mails to unknown recipients using e-mail addresses indiscriminately collected on the internet (e.g. by use of a web crawler) violates the DPA, regardless of whether such e-mails provide for an opt-out.

Conditions for direct marketing by e-mail to corporate subscribers

The same conditions apply as for direct marketing by e-mail to individual subscribers.

Exemptions and other issues

The *similar products and services exemption* applies under the revised Unfair Competition Act ("opt-out"). However, pursuant to the prevailing legal doctrine in Switzerland, the exemption only applies if indeed a contract has been formed; it is not sufficient that the contact details have been collected in connection with a contract negotiation (which did not result in a contract). Furthermore, according to the prevailing legal doctrine, the exemption only applies if the recipient has been informed of the possibility to refuse e-mails at the time when the contract has been formed or during follow-up interactions related to the contract (e.g. deliveries, invoices). Conversely, the exemption would not apply if a business were to collect contact information in the context of a product sale, but provide the "opt-out" information only later on by separate e-mail without such context. Consequently, there is in practice only a very narrow field of application for the *similar products and services exemption* under Swiss law. In most cases, businesses will find it easier and safer to obtain

prior consent (e.g., by use of an appropriate provision in the general terms and conditions), which should also help compliance with the Swiss Robinson List (see above).

The Swiss Unfair Competition Act also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) a simple means for refusing further e-mails free of charge (e.g., a link to click on for opting out) is not provided with each e-mail.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is, in principle, not permitted to make direct marketing calls to individual subscribers who: (i) have previously objected to such calls; or (ii) are listed in the telephone directory with the corresponding phone number as not wishing any communications to such number for the purpose of direct marketing (since 1 April 2012, this is expressly regulated by the Swiss Unfair Competition Act, which introduced the concept of an official Robinson List, see above). The necessary contact information may be obtained and used only in compliance with the DPA, for example, if the subscriber made it publicly available (e.g. by having it listed in the telephone directory), or has provided it and implicitly or explicitly agreed to its use for marketing purposes.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The same conditions apply as for direct marketing by telephone to individual subscribers.

Exemptions and other issues

Calls can be made to a subscriber who has consented to receiving such calls.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Pursuant to the Swiss Unfair Competition Act, sending unsolicited mass direct marketing fax messages is only allowed if: (i) the recipient has provided his prior consent ("opt-in"); (ii) the sender's address is correct; and (iii) the recipient is given a simple means of refusing further faxes free of charge (except for the costs of transmitting the refusal) with each communication. The recipient's consent does not necessarily have to be in writing.

Conditions for direct marketing by fax to corporate subscribers

The same conditions apply as for direct marketing by fax to individual subscribers.

Exemptions and other issues

The *similar products and services exemption* applies. However, pursuant to the prevailing legal doctrine in Switzerland, the exemption only applies if a contract has indeed been formed; it is not sufficient that the contact details have been collected in connection with a contract negotiation (which did not result in a contract). Furthermore, according to the prevailing legal doctrine, the exemption only applies if the recipient has been informed of the possibility to refuse e-mails at the time when the contract has been formed or during follow-up interactions related to the contract (e.g. deliveries, invoices). Conversely, the exemption would not apply if a business were to collect contact information in the context of a product sale, but provide the "opt-out" information only later on by separate e-mail or fax without such context. Consequently, there is only a very narrow field of application for the *similar products and services exemption*. In most cases, businesses will obtain prior consent. Since 1 April 2012, pursuant to a new provision of the Swiss Unfair Competition Act that introduced the concept of an official Robinson List, prior consent is necessary also for those recipients whose entry in the official telephone directory contains an opt-out mark for the corresponding phone number.

Ukraine.

Contributed AstapovLawyers International Law Group

General | Data Protection Laws

National Legislation

General data protection laws

Ukraine is not an EU Member State and therefore has not implemented the *Data Protection Directive*. However, the Law of Ukraine "On Personal Data Protection" (No.2297-VI, dated 1 June 2010) (the "**OPDP Law**") was passed by the Parliament in 2010 and is similar to the *Data Protection Directive*. The OPDP Law was recently amended by the Law on Amending the OPDP Law, which became effective 20 December 2012.

Entry into force

The provisions of the OPDP Law came into force on 1 January 2011.

National Regulatory Authority

Details of the competent national regulatory authority

State Service of Ukraine on Personal Data Protection (the "**State Service**")
15 Maryny Raskovoi str.
02660 Kyiv, Ukraine

Notification or registration scheme and timing

All personal databases are subject to state registration provided by the State Service. The database owner has to notify the State Service of the name of the database, its location, the aim of processing and the names of database processors, if any. The respective database should be recorded in the State Register of Databases and an approval (Registration Certificate) issued within 30 days of the notification.

Additionally, a database owner has to notify the State Service on each change of information provided for the purposes of database registration within 10 days of such change taking place.

Exemptions

A database owner is released from the obligation to register the database if: (i) maintenance of the database is related to the support and implementation of employment relations; or (ii) the database contains information on members of non-governmental organisations, religious organisations, professional organisations or political parties.

Appointment of a data protection officer

All legal entities must appoint a data protection officer or have a compliance department responsible for data protection matters.

Personal Data

What is personal data?

The OPDP Law defines personal data as information on natural persons, who are identified or identifiable.

Personal data (unless anonymised) is treated as "information with restricted access" for the purposes of the Laws of Ukraine "On Information" and "On Access to Public Information"(No. 265-XII, dated 2 October 1992) (the "**Information Laws**").

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

Personal data may be processed: (i) with the *data subject's* consent; (ii) where such processing is to be carried out in accordance with law and the database owner's specific authorisation; (iii) for the conclusion and execution of an agreement transaction when the *data subject* is party to such a transaction or when such a transaction is concluded in favour of the *data subject*, or for activities that have been completed prior to the transaction at the request of the *data subject*; (iv) for the protection of the vital interests of the *data subject*; or (v) where necessary to protect the legitimate interests of the owners of the personal data, or third parties, except when the *data subject* requires processing of his/her personal data to cease and the needs of personal data protection prevail over such interest.

The general principles of data processing are similar to the *standard conditions for processing personal data*.

Where the aim of the processing changes, new consent must be obtained from the *data subject*.

However, as personal data is also "information with restricted access" for the purposes of the Information Laws (see above) it is only possible to disclose such information: (i) where provided for by law; or (ii) for national security reasons or to protect human rights. It may be stated by Ukrainian laws that certain personal data should not be treated as "information with restricted access" where there is a need to ensure that the information is publicly available.

The OPDP Law is not applicable to the processing of personal data by natural persons for personal or domestic needs, or by a person with a literary or artistic engagement, including journalists, for professional purposes.

When processing personal data the data protection officer or compliance department of the legal entity must: (i) inform employees of the requirements related to data protection; (ii) oversee data processing by the respective employees; (iii) oversee the processing of enquiries related to personal data; (iv) ensure access to personal data; and (v) inform the owner or manager of the personal database of any breach of established procedures for personal data processing, and on measures necessary to process personal data in accordance with the law.

Are there any formalities to obtain consent to process personal data?

The consent of the *data subject* must be in a documentary form, for example in writing. The electronic consent of the *data subject* must contain an electronic signature under the Law of Ukraine "On Electronic Digital Signature" (852-IV, dated 22 May 2003).

Sensitive Personal Data

What is sensitive personal data?

Under the OPDP Law, sensitive personal data means the *standard types of sensitive personal data*.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed only if conditions broadly similar to the *standard conditions for processing sensitive personal data* are satisfied.

Are there any formalities to obtain consent to process sensitive personal data?

The consent of the *data subject* to processing of sensitive personal data must be given in documentary form, for example in writing. The electronic consent of the *data subject* must contain an electronic signature under the Law of Ukraine "On Electronic Digital Signature" (852-IV, dated 22 May 2003).

Scope of Application

What is the territorial scope of application?

The OPDP Law does not contain any express provisions on its territorial effect. It is, therefore, likely to apply to processing of personal data: (i) in Ukraine; or (ii) which relates to Ukrainian citizens or residents regardless of where the data operator is established.

Who is subject to data protection legislation?

The OPDP Law uses the terms "database owner" and "database processor".

The database owner is broadly equivalent to the concept of a *data controller*. It means a person who: (i) has a right to process the personal data based on the consent of *data subject* or pursuant to specific provisions of Ukrainian laws; (ii) confirms the purpose of processing in the database; and (iii) determines the scope of data and the processing procedure.

In contrast, a *data processor* is a person who processes personal data either on behalf of a database owner or where required to do so by Ukrainian laws. It is therefore similar to the concept of a *data processor* but not identical.

Are both manual and electronic records subject to data protection legislation?

The OPDP Law applies to "personal databases". These are compilations of personal data recorded in electronic and/or manual form.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation for damage, including moral damage for upset or distress

Fair processing information

The *data subject* has to be notified in writing, within 10 days of the collection of personal data commencing, on: (i) the identity of the owner of the personal data; (ii) the composition and contents of the collected personal data; (iii) the rights of the *data subject* and the purposes of the personal data collection; and (iv) the persons to whom the data has been transferred.

Rights to access information

The OPDP Law gives *data subjects* the right to obtain, upon request, information on: (i) the location of the database which contains their data; (ii) the name and location of the database owner; (ii) conditions of access to the database; and (iv) the third parties or other recipients to whom the data is transferred.

Data subjects also have a right to access their personal data in the relevant database. *Data subjects* have the right to know whether their personal data is being stored in a personal database and to know the scope of personal data held. Such answer must be provided by the database owner (processor) not later than 30 calendar days from the date of request, unless otherwise provided by Ukrainian laws. A subject access request is free of charge.

Objection to direct marketing

No rights to object to direct marketing have been implemented into the OPDP Law.

Other rights

The *data subject* may file a claim: (i) objecting to data processing by state authorities or local government bodies; or (ii) seeking the rectification or deletion of personal data by the database owner.

The *data subject* is also entitled to: (i) restrict the processing of their personal data; (ii) withdraw consent in relation to the processing of their personal data; (iii) know the mechanics of the automated processing of personal data; and (iv) be protected against automated decisions that have legal effect.

The *data subject* also has a right to protection from illegal processing, loss, deletion, and damage of personal data, as well as from the provision of unreliable information which discredits his/her honour, dignity and business reputation.

Security

Security requirements in order to protect personal data

The OPDP Law provides that the database owner must ensure personal data is kept secure but does not specify any particular measures. However, the State Service has issued guidance stating that security measures should include matters such as an assessment of processing, implementation of a controlling system and evaluation of performance.

Thus, the State Service generally refers to the *general data security obligations* but does not provide an obligation to apply specific security requirements.

Specific rules governing processing by third party agents (processors)

The database owner must ensure that any data processing carried out by a database processor is under a written agreement.

Notice of breach laws

No.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The transfer of a database related to personal data to non-residents is allowed, provided that the relevant state ensures appropriate protection of personal data. Grounds for such transfer are set forth by Ukrainian law or international treaties of Ukraine.

Members of the EEA, as well as states which have signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, are deemed states which ensure an appropriate level of personal data protection. States included on the list approved by the Cabinet of Ministers of Ukraine are also deemed to provide such protection.

Personal data can be transferred to non-residents also if: (i) consent for the transfer is obtained from the *data subject*; (ii) the transfer is necessary to conclude and execute a transaction between an owner of personal data and a third party in favour of *data subject*; (iii) the transfer is necessary to protect the vital interests of the *data subject*; (iv) the transfer is necessary to protect public interest, establishment, execution and provision of a legal claim; or (v) the owner of the database provides appropriate guarantees in relation to non-interference in the personal and family life of the *data subject*.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no obligation to obtain the approval of the State Service.

Use of binding corporate rules

The OPDP Law allows professional organisations to rely on *binding corporate rules* in order to obtain effective protection of personal data for transfers of personal data outside Ukraine, subject to approval by the State Service.

Enforcement

Sanctions

The law on administrative liability for the breach of provisions of the OPDP Law became effective on 1 January 2012. Under this law, fines of up to EUR 1,700 can be issued for non-compliance with the mandatory database registration requirement.

Personal data is also deemed to be "confidential information". Under article 182 of the Criminal Code of Ukraine the illegal collection, storage, use, disposal dissemination and change of confidential information relating to a certain person attracts penalties including: (i) fines from UAH 8,500 to 17,000; (ii) corrective labour for up to two years; (iii) arrest for up to six months; or (iv) up to three years' imprisonment.

Practice

In practice, the State Service normally first issues a warning requesting that the violation of the OPDP Law ceases. Administrative fines may then be imposed if the guilty party does not comply with this warning. It is rare for criminal liability to result from cases related to the illegal disposal of confidential information.

Enforcement authority

The courts impose administrative fines on a database owner based on notices on administrative offences served by the State Service.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

Ukraine is not an EU Member State and, therefore, has not implemented the *Privacy and Electronic Communications Directive*. Regulations on direct marketing by email, fax and telephone are stated in other laws such as Law of Ukraine "On Advertising" (No. 270/96-BP dated 3 July 1996), Law of Ukraine "On Consumer Protection" (No. 1023-XII dated 12 May 1991) and the Resolution of Cabinet of Ministers of Ukraine on Approval of Rules on Provision and Receipt of Telecommunication Services (No.295 dated 11 April 2012).

Cookies

Conditions for use of cookies

There are no special rules for cookies.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Under the laws of Ukraine, sending direct marketing electronic messages without a consumer's consent is forbidden.

Conditions for direct marketing by e-mail to corporate subscribers

The laws of Ukraine relating to direct marketing by email do not apply to corporate subscribers.

Exemptions and other issues

None.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

Repetitive direct marketing calls to a consumer are prohibited without that consumer's consent.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The laws of Ukraine relating to direct marketing by telephone do not apply to corporate subscribers.

Exemptions and other issues

None.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

Under the laws of Ukraine, sending directive marketing fax messages without a consumer's consent is forbidden.

Conditions for direct marketing by fax to corporate subscribers

The laws of Ukraine relating to direct marketing by fax do not apply to corporate subscribers.

Exemptions and other issues

None.

United Kingdom.

General | Data Protection Laws

National Legislation

General data protection laws

The Data Protection Act 1998 (the "**DPA**") which implements the *Data Protection Directive*.

Entry into force

The majority of the provisions of the DPA came into force on 1 March 2000.

National Regulatory Authority

Details of the competent national regulatory authority

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
United Kingdom

www.ico.gov.uk

Notification or registration scheme and timing

Personal data may not be processed by a *data controller* unless it has submitted a notification to the Information Commissioner or its processing is exempt. No approval is required. Notification costs £35 or £500 depending on the size and nature of the *data controller*. The notification must occur prior to the first processing of personal data.

Exemptions

Every *data controller* who is processing personal data must notify the Information Commissioner unless they are exempt. Exemptions apply in respect of: (i) staff administration; (ii) advertising and marketing etc. of the *data controller's* business; (iii) accounts and records of the *data controller* or its customer/supplier; (iv) certain processing relating to non-profit-making organisations; and (v) maintenance of a public register.

Appointment of a data protection officer

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

Personal Data

What is personal data?

The DPA defines personal data to mean any data relating to living individuals who can be identified from: (i) the data; or (ii) the data and other information which is in, or is likely to come into, the possession of the *data controller*, including expressions of opinion and indications of the *data controller* in respect of that individual. This definition is therefore closely based on the *standard definition of personal data*.

The requirement that personal data "relate to" an individual was considered by the Court of Appeal in the case of *Durant v Financial Services Authority*, which suggested that there are two notions which may be used to help decide whether information could be considered to be "personal data". The first is whether the information is "biographical in a significant sense, that is, going beyond the recording of the putative *data subject*'s involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised". The second is that the information should have the *data subject* as its focus rather than some other person or event such as an investigation into some other body's conduct. The court also held that: "In short, [personal data] is information that affects his privacy, whether in his personal or family life, business or professional capacity."

The decision in *Durant* was a controversial one, and has attracted considerable criticism. The Information Commissioner has subsequently adopted guidance that adopts a much broader approach to this definition that is quite closely based on the *Opinion on Personal Data*.

Is information about legal entities personal data?

No. However, information about sole traders and partnerships is personal data as they are treated as individuals.

What are the rules for processing personal data?

Personal data may be processed if the *standard conditions for processing personal data* are met. In practice, the legitimate interests condition is frequently relied upon as grounds for processing non-sensitive personal data.

The DPA contains exemptions for certain types of processing. For example, processing for domestic purposes is largely exempt from the provisions of the DPA.

Are there any formalities to obtain consent to process personal data?

There are no formalities to obtain consent under the DPA to process personal data. Consent can be express, written, oral or implied. However, obtaining consent from employees can be difficult as, in some cases, it may be hard to demonstrate that consent has been freely given by the employee.

Sensitive Personal Data

What is sensitive personal data?

Under the DPA, sensitive personal data includes both: (i) the *standard types of sensitive personal data*; and (ii) information about criminal offences or criminal proceedings. In *Murray v Big Pictures,* the court held that a photo could be sensitive personal data if it revealed the ethnic origin of the persons in the picture.

Are there additional rules for processing sensitive personal data?

Sensitive personal data may be processed if the *standard conditions for processing sensitive personal data* are met. A range of additional processing conditions are set out both in the DPA and in a separate Order, including processing for equal opportunities monitoring, regulatory investigations, research and political activities.

Are there any formalities to obtain consent to process sensitive personal data?

Not as such. However, the DPA states that "explicit" consent is required, so it is unlikely that implied consent would be sufficient. Similarly, while consent can be written or oral, in many cases written consent will be desirable.

Scope of Application

What is the territorial scope of application?

The DPA applies the *standard territorial test*.

Who is subject to data protection legislation?

The DPA applies to *data controllers*. *Data processors* are not subject to the DPA.

Are both manual and electronic records subject to data protection legislation?

Yes. The DPA applies to "data" - i.e. information processed by automatic equipment or stored on a "relevant filing system". It also applies to information recorded with the intention that it be added to automatic equipment or a relevant filing system.

A relevant filing system is a set of information that is: (i) structured by reference to individuals or by reference to criteria relating to individuals; and (ii) makes specific information relating to that individual readily accessible. In *Durant v Financial Services Authority*, the Court of Appeal suggested that a relevant filing system must be "of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system".

Finally, all recorded information is treated as data in the hands of a UK public authority.

Rights of Data Subjects

Compensation

Data subjects have a right to compensation if they suffer damage or damage and distress. The case of *Johnson v Medical Defence Union* indicates that the term "damage" only extends to pecuniary loss, though this decision was criticised by the Court of Appeal in *Murray v Big Pictures*.

Fair processing information

A *data controller* must provide the *fair processing information* to *data subjects*. If the personal data has been obtained from a third party rather than the *data subject* then the *fair processing information* need not be provided if: (i) it would involve disproportionate effort; or (ii) the processing is necessary for compliance with a legal obligation.

There is no obligation in the DPA to provide this information in English, though it may be difficult to show that the information has been fairly provided if it is not in a language the *data subject* is familiar with. There is no obligation to refer to the DPA itself in any *fair processing information.*

Rights to access information

Data subjects may obtain their *subject access information* by written request to *data controllers*. A subject access request costs £10 (subject to certain variations for particular types of subject access request). The scope of this right was clarified in *Ezsias v Welsh Ministers* which stated a *data controller* need only use "reasonable and proportionate" efforts

to find personal data in response to a subject access request. There are also a range of statutory exceptions for certain types of personal data.

Objection to direct marketing

A *data subject* may require in writing that a *data controller* stop processing his personal data for direct marketing purposes. The *data controller* must then cease such processing within a reasonable period.

Other rights

In certain cases, the *data subject* may ask the court to order the *data controller* to rectify, block, erase or destroy the data. An individual may in writing require that the *data controller* cease processing either generally or for a specified purpose or in a specified manner data concerning the individual if such processing is likely to cause substantial damage or distress to the individual or a third party and that damage/distress would be unwarranted. In certain cases, a *data subject* may object to decisions being taken about him based solely on automatic processing.

Security

Security requirements in order to protect personal data

The DPA only refers to the *general data security obligations* and does not contain any specific security requirements. However, the Information Commissioner has issued a range of guidance which, amongst other things, recommends the use of encryption (especially on mobile devices such as laptops).

Specific rules governing processing by third party agents (processors)

The processing of personal data by a *data processor* must be in accordance with a written contract containing the *standard processor obligations*.

Notice of breach laws

The DPA does not contain any obligation to inform the Information Commissioner or *data subjects* of a security breach. However, the Information Commissioner has issued guidance stating that he expects to be informed of any serious security breaches on a voluntary basis.

Specific notice of breach laws apply to the electronic communications sector in accordance with the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*. Moreover, *data controllers* in certain sectors may be required to inform sectoral regulators of any breach (for example, financial services firms may be required to inform the Financial Services Authority of any breach).

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

The DPA contains a restriction on *transborder dataflows*. Transfers can take place if the transfer satisfies the *standard conditions for transborder dataflow*. Alternatively the *data controller* can rely on its own assessment of whether the personal data will be adequately protected after it has been transferred outside of the EEA.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no obligation to notify or obtain the consent of the Information Commissioner to any *transborder dataflows*. In particular, there is no obligation to notify the Information Commissioner or obtain his consent to use the *Model Contracts*.

Use of binding corporate rules

The Information Commissioner has approved the use of *binding corporate rules* in the UK and is a member of the mutual recognition club. To date, the Information Commissioner has approved *binding corporate rules* from GE, Philips, Atmel, Accenture, Hyatt, JP Morgan, BP, IMS Health, Spencer Stuart, CareFusion. First Data, eBay, Novo Nordisk, Linklaters, Citigroup, Intel and American Express.

Enforcement

Sanctions

The Information Commissioner can issue an Enforcement Notice for breach of the data protection principles. Failure to comply with that Enforcement Notice is a criminal offence, punishable by unlimited fines (including for directors) but not jail terms.

The Information Commissioner also has the power to impose monetary penalty notices (an administrative fine) for up to £500,000 if: (i) there is a serious breach of the data protection principles; (ii) this is likely to cause substantial damage or substantial distress; and (iii) the breach is deliberate or reckless.

Failure to notify and the unlawful obtaining or disclosing of personal data are criminal offences. These offences are currently punishable by unlimited fines (including for directors) but not jail terms. However, the Government has the power to increase the sentence for unlawfully obtaining or disclosing personal data to two years' imprisonment.

Finally, the Information Commissioner sometimes asks for public undertakings from organisations that have committed less serious breaches of the data protection principles. These undertakings do not have any statutory power but do serve to "name and shame" the organisation and act as an admission of guilt should further breaches occur.

Practice

20,080 new complaints were received by the Information Commissioner in the year ending March 2012. Over a quarter of the complaints related to subject access requests, with other common complaints including inaccurately recorded data, disclosures of data, direct marketing phone calls and security breaches.

In the year ending December 2012 he issued 25 fines (monetary penalty notices) totalling £3.12 million. Most of the fines were as a result of security breaches but he also fined a financial organisation £50,000 for failing to keep accurate records and fined a firm £440,000 for sending "spam texts". He also asked for 31 undertakings and issued three enforcement notices.

There were six prosecutions in the year ending December 2012. Three prosecutions related to the unlawful obtaining or disclosing of personal data. The other three prosecutions were for failure to make a notification to the Information Commissioner.

Enforcement authority

The Information Commissioner can issue monetary penalty notices himself. Alternatively, he can issue Enforcement Notices, the breach of which is a criminal offence. However, the actual prosecution for a criminal offence must be brought before the UK criminal courts.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "**PECR**") which implement the *Privacy and Electronic Communications Directive.* These regulations came into force on 11 December 2003.

The PECR was amended on 26 May 2011 to implement the amendments to the *Privacy and Electronic Communications Directive* made by the *Citizens' Rights Directive*.

Cookies

Conditions for use of cookies

Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user.

The PECR expressly states that consent can be given through browser settings. There is no express requirement for consent to be "prior" to the use of a cookie.

Regulatory guidance on the use of cookies

The Information Commissioner has issued detailed guidance on the use of cookies, the most recent iteration of that guidance being issued in May 2012. It states that current browser settings are not sufficient to provide consent but that consent is a flexible concept and can be obtained in other ways.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

It is only possible to send direct marketing e-mails to individual subscribers if they consent.

Conditions for direct marketing by e-mail to corporate subscribers

The restrictions on e-mail marketing in the PECR do not apply to corporate subscribers (including individuals at corporates). However, the CAP Code does require consent for the marketing of personal items to individuals at corporate subscribers. The CAP Code is a self-regulatory code of conduct for advertisements.

Exemptions and other issues

It is permitted to send e-mail for the purposes of direct marketing if the *similar products and services exemption* applies. For this exemption to apply the recipient's details only need to have been collected in connection with the sale or negotiation for sale of products and services. There is no need for an actual contract to have been formed.

The PECR also prohibits direct marketing e-mails from being sent if: (i) the identity of the sender is disguised or concealed; or (ii) if an opt-out address is not provided. The sender must also include the *eCommerce information*.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to individual subscribers who have either: (i) previously objected to such calls; or (ii) are listed on the Telephone Preference Service.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

It is not permitted to make direct marketing calls to corporate subscribers who have either: (i) previously objected to such calls; or (ii) are listed on the Telephone Preference Service.

Exemptions and other issues

Calls can be made to a subscriber on the Telephone Preference Service if they have consented to receiving such calls. The recipient should be told the name of the person responsible for the direct marketing call and, on request, an address or telephone number where he can be reached free of charge.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

It is not permitted to send direct marketing faxes to individual subscribers without their consent.

Conditions for direct marketing by fax to corporate subscribers

It is not permitted to send direct marketing faxes to corporate subscribers who have either: (i) previously objected to such faxes; or (ii) are listed on the Fax Preference Service.

Exemptions and other issues

Faxes can be sent to a subscriber on the Fax Preference Service if they have consented to receiving such faxes. The recipient should be told the name of the person responsible for the direct marketing fax and an address or telephone number where he can be reached free of charge.

Vietnam.

Contributed by Allens

General | Data Protection Laws

National Legislation

General data protection laws

There is no consolidated law on data protection in Vietnam. Instead, the relevant framework is derived from a number of different laws. Relevant provisions can be found in the Constitution, the Civil Code (Law No. 33/2005/QH11), the Law on Protection of Consumers' Rights (Law No. 59/2010/QH12), the Law on E-Commerce (Law No. 51/2005/QH11), the Law on Information Technology (Law No. 67/2006/QH11), the Law on Insurance Business (Law No. 24/2000/QH11 as amended by Law No. 61/2010/QH12), and the Law on Credit Institutions (Law No. 47/2010/QH12). Primary legislation tends to be generally drafted leaving its precise application open to interpretation. This interpretation is sometimes clarified by detailed regulations, but not in all cases. Therefore, application of the law to a particular set of facts is not always clear.

Entry into force

The laws referred to above came into effect on a number of different dates.

National Regulatory Authority

Details of the competent national regulatory authority

Not applicable.

Notification or registration scheme and timing

There is no notification or registration scheme for the collection, use or disclosure of personal data.

Exemptions

Not applicable.

Appointment of a data protection officer

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

Personal Data

What is personal data?

Under Vietnamese law, the scope of the definition of personal data is not fixed and varies depending on the particular law. The only regulation containing a clear definition is Decree 64 on application of IT in State Bodies, in which personal data is defined to mean information which is adequate to accurately identify the identity of a *data subject*, covering at least one of the following types of information: full name, date of birth, profession, title, contact address, e-mail address, telephone number, ID number and passport number. Personal secrets include medical records, tax payment dossiers, social insurance card numbers, credit card numbers and other personal secrets.

Is information about legal entities personal data?

No.

What are the rules for processing personal data?

As noted above, there is no consolidated law on data protection in Vietnam. The relevant framework is derived from a number of different sources. The Civil Code of Vietnam provides that a *data subject's* right to privacy shall be respected and protected by law. The collection and publication of information and data about the private life of a *data subject* must only occur with the consent of the *data subject* or, where the *data subject* has died, has lost the capacity for civil acts or is not yet 15 years of age, the consent of a parent, spouse, adult child or representative of that person must be obtained, except where the collection and publication of information and data are required pursuant to a decision of an authorised State body.

The Civil Code of Vietnam also provides that the mail, telephone, electronic mail communications and other forms of electronic information of a *data subject* must be protected and kept confidential and that the control of mail, telephone, electronic mail communications and other forms of electronic information of a *data subject* may only take place in circumstances stipulated by law and subject to a decision issued by an authorised State body.

The Law on Information Technology specifically regulates the processing of personal data in network environments. Organisations and individuals collecting, processing and using the personal data of *data subject* in a network environment must obtain consent from the *data subject*, unless otherwise stipulated by law. Organisations and individuals collecting,

processing and using personal data of another person have the following responsibilities: (i) to notify such person of the form, scope, place and purpose of the collection, processing and use of his or her personal data; (ii) to use the collected personal data for proper purposes and to store such information only for a certain period as stipulated by law or as agreed upon by the two parties; (iii) to take necessary managerial or technical measures to ensure that the personal data shall not be lost, stolen, disclosed, modified or destroyed; (iv) to immediately take necessary measures upon receipt of a request for re-examination, correction or cancellation; and (v) not to supply or use relevant personal data until such information is corrected.

Under the Law on Information Technology, organisations and individuals shall be entitled to collect, process and use personal data of other *data subjects* without the consent of the *data subject* in the following circumstances: (i) signing, modifying or performing contracts for use of information, products or services in a network environment; (ii) pricing or calculating charges for use of information, products or services in the network environment; and (iii) performing other obligations in accordance with law.

Similar responsibilities are also provided under the Law on Protection of Consumers' Rights: (i) to provide, in advance, clear and public notice to consumers regarding the purpose of collating and using their personal data; (ii) to use personal data appropriately in accordance with the purpose notified to consumers, and to obtain the consent of the *data subject* before collating and using their personal data; (iii) to ensure the safety, accuracy and completeness of the personal data when collating, using or transferring personal data; (iv) to update and amend personal data on becoming aware that they are inaccurate, or to take measures to enable *data subjects* to update and amend their personal data; and (v) to transfer personal data to a third party only where the *data subject* consents, unless otherwise authorised by law.

Are there any formalities to obtain consent to process personal data?

There are no specific formalities to obtain consent from the *data subject*.

Sensitive Personal Data

What is sensitive personal data?

Sensitive personal data is not defined under Vietnamese law.

Are there additional rules for processing sensitive personal data?

No.

Are there any formalities to obtain consent to process sensitive personal data?

No.

Scope of Application

What is the territorial scope of application?

All the Vietnamese laws apply to activities conducted partly or wholly in the territory of Vietnam.

Who is subject to data protection legislation?

General principles relating to the protection of personal data apply to individuals, companies and State bodies.

Vietnamese law does not use the terms *data controller*, *data processor* and *data subject*. However, for the purpose of consistency, we use such terms in this summary.

Are both manual and electronic records subject to data protection legislation?

Yes. There is no specific distinction between manual and electronic records under Vietnamese law.

Rights of Data Subjects

Compensation

Under the Civil Code, if personal data rights are infringed the *data subject* is entitled to demand or request a competent body or person to compel the infringing party to compensate the *data subject*.

Fair processing information

Under the Law on Information Technology, an organisation must notify the person whose data are processed of the form, scope, place and purpose of the collection, processing and use of his or her personal data.

In addition, the collection of personal data must only occur with the consent of the *data subject*. As a result, if there is a request by the *data subject* for information about the use of data for the purposes of the *data subject* providing consent to the collection of the data, the person collecting the data is required to provide this information.

Rights to access information

The right of *data subjects* to access personal data about themselves is not generally provided under Vietnamese law.

Objection to direct marketing

The consent of the *data subject* is required in order to use personal data for the purposes of direct marketing.

Other rights

If personal data rights are infringed, the *data subjects* have the right to correct the data themselves or demand or request a competent body to compel the infringing party to terminate the infringing act. This means that if personal data are collected without consent, or are misused, the *data subject* may request the person collecting the data to stop processing and/or delete such personal data. Specifically, in the case of the storage and supply of personal data in a network environment, the *data subject* is entitled to request the organisations/persons storing such data to verify, correct or delete the data.

Security

Security requirements in order to protect personal data

Under the Law on Information Technology, organisations must take necessary managerial or technical measures to ensure that the personal data shall not be lost, stolen, disclosed, modified or destroyed.

Generally, there are no other specific general statutory security requirements for the protection of personal data in Vietnam. Instead, the law broadly requires that the lawful personal data of an organisation or *data subject* being exchanged, transmitted or stored in the network environment shall be kept confidential. However, in some particular areas such as finance or in the case of government or political organisations, other specific data security requirements may also exist.

Specific rules governing processing by a third party agents (processors)

There are no specific rules governing processing of personal data by a third party agent.

Notice of breach laws

There are no specific requirements to inform a regulator and/or *data subjects* of data security breaches.

Transfer of Personal Data to Third Countries

Restrictions on transfers to third countries

There are no specific restrictions on the transfer of personal data to third countries.

Notification and approval of national regulator (including notification of use of Model Contracts)

There is no national privacy regulator in Vietnam.

Use of binding corporate rules

There is no ability to use *binding corporate rules* in respect of transfers to Third Countries.

Enforcement

Sanctions

Infringement of privacy laws may lead to the following administrative fines or criminal penalties: (i) administrative fines of between USD 50 and 150 for the acts of publishing personal data without the consent of the *data subject*; (ii) administrative fines of between USD 150 and 250 for the acts of failing to keep necessary management and technical measures to ensure the safety of personal data of other persons or supplying personal data of other persons to a third party in a network environment; and (iii) criminal penalties of up to two years' imprisonment for the act of infringement of other persons' rights to privacy or other circumstances arising in relation to the access or interception of communications (mail, telephone and/or telegraphic communications) without the consent of the *data subject*.

Practice

There have been some cases of regulators imposing administrative fines for breaches of personal privacy, mostly in a network environment. However, privacy laws are not regularly enforced. There is no exact statistic on the number of enforcement actions taken in the last 12 months and the majority of enforcement actions are not publicly disclosed.

Enforcement authority

The regulator with jurisdiction over the applicable regulation is responsible for enforcing breaches of that regulation. Courts have authority to enforce civil or criminal sanctions.

ePrivacy I Marketing and cookies

National Legislation

ePrivacy laws

There is no specific ePrivacy law in Vietnam. However, the Law on Information Technology and Law on Electronic Transactions contain some provisions that address ePrivacy issues.

Cookies

Conditions for use of cookies

The use of cookies is not specifically regulated under Vietnamese law. However, personal data collected via the use of cookies are subject to Vietnamese privacy laws in the same manner as other personal data.

Regulatory guidance on the use of cookies

Not applicable.

Marketing by E-mail

Conditions for direct marketing by e-mail to individual subscribers

Decree 90 dated 13 August 2008 on Anti-Spam as amended (Decree 90) requires that any service provider sending advertising emails must satisfy all the following conditions: (i) the service provider must have a website using the "dot vn" domain name and a server for sending advertising emails which is set up in Vietnam; (ii) the service provider must have a system for the receipt and processing of opt-out requests; (iii) the service provider must have been issued with a management code number by the Ministry of Information and Communication.

The following conditions must also be satisfied upon sending advertising emails to individual subscribers: (i) advertising emails must be sent only after obtaining the prior express consent of recipients; (ii) advertising emails must not be sent after receiving opt-out requests from recipients; (iii) advertising emails must only be sent from electronic addresses and systems which conform with regulations of the Ministry of Information and Communications; (iii) when sending advertising emails, a copy must be concurrently sent to the technical system of the Ministry of Information and Communications; (iv) no more than one advertising message of similar content must be sent to an email address within 24 hours, unless otherwise agreed upon with recipients; and (v) advertising contents must comply with the advertising law.

Conditions for direct marketing by e-mail to corporate subscribers

The rules are the same as for individual subscribers.

Exemptions and other issues

Decree 90 provides for other requirements. In particular, advertising service providers and advertisers must provide information such as name, telephone, email address, geographical address, and website (if any). This information must be expressly set out in the email and must be provided immediately before the select function permitting the recipient to opt-out of email marketing.

Where necessary, an opt-out mechanism must be provided by the advertising service provider so that the recipient can opt-out of marketing relating to one product or a group of products. The opt-out mechanism may be provided by way of a website, email or telephone. Upon receiving an opt-out request, the advertiser or advertising service provider must immediately send confirmation of its receipt of the opt-out request and stop sending the applicable type of opt-out advertising emails to the recipient.

Marketing emails must be marked as commercial in their subject field. If the emails come from advertising service providers, this must be accompanied by the management code number of the sender of the email.

Marketing by Telephone

Conditions for direct marketing by telephone to individual subscribers (excludes automated calls)

There are no regulations that govern direct marketing to individuals by telephone. However, direct marketing by text message to telephone subscribers is subject to the same conditions as email marketing referred to above. In addition, sending marketing text messages is only allowed between the hours of 7.00 and 22.00, unless otherwise agreed by the recipients.

Conditions for direct marketing by telephone to corporate subscribers (excludes automated calls)

The rules are the same as for individual subscribers.

Exemptions and other issues

Not applicable.

Marketing by Fax

Conditions for direct marketing by fax to individual subscribers

There are no regulations that specifically govern direct marketing to individuals by fax. While the position is not entirely certain, it is possible that the obligations relating to direct marketing by text messages may apply to direct marketing by fax. However, this position has not yet been considered by any regulator or court.

Conditions for direct marketing by fax to corporate subscribers

The rules are the same as for individual subscribers.

Exemptions and other issues

Not applicable.

Glossary.

binding corporate rules	means a set of binding rules adopted by an organisation and approved by national data protection regulators to ensure the protection of personal data in multiple jurisdictions.
Citizens' Rights Directive	means Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
data controller	means the person which alone or jointly with others determines the purposes and means of the processing of personal data (Article 2(d), *Data Protection Directive*).
data processor	means a person which processes personal data on behalf of a *data controller* (Article 2(e), *Data Protection Directive*). Further information about this concept is in the Article 29 Working Party's Opinion 1/2010 on the concepts of "controller" and "processor" (WP 171).
Data Protection Directive	means Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
data subject	means an individual about whom personal data is being processed.
eCommerce information	means: (a) clear identification of commercial communications, and unsolicited commercial communications, as such; (b) clear identification of the natural or legal person on behalf of whom a commercial communication is made; (c) promotional offers, competitions and games are clearly identified (including conditions for participation) and the relevant email does not encourage recipients to visit websites that contravene these requirements.
fair processing information	means the provision of information about: (a) the identity of the *data controller* and of his representative, if any; (b) the purposes of the processing for which the data are intended; and (c) any further information in so far as such further information is necessary, having regard to the circumstances in which the data are collected, to guarantee fair processing (Article 10, *Data Protection Directive*).
general data security obligations	means the obligation to implement appropriate technical and organisational measures to protect personal data having regard to the state of the art, the risks represented by the processing and the nature of the data to be protected (Article 17(1), *Data Protection Directive*).
Model Contracts	means the contractual clauses set out in Commission Decision C(2010) 593, Commission Decision C(2004) 5271 and Commission Decision C(2001) 1539.
Opinion on Personal Data	means the Article 29 Working Party's Opinion 4/2007 on the concept of personal data (WP 136).
Privacy and Electronic Communications Directive	means Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
similar products and services exemption	applies where a person collects a customer's e-mail details in connection with a sale of a product or service and uses these contact details for direct marketing of its own similar products or services provided that customers are given the opportunity to object to such use of electronic contact details when they are collected and on the occasion a message is sent.
standard conditions for processing personal data	means the processing satisfies the general principles for data processing and is: (a) carried out with the *data subject's* consent; or (b) necessary for the performance of a contract with the *data subject*; or (c) necessary for compliance with a legal obligation; or (d) necessary in order to protect the vital interests of the *data subject*; or (e) necessary for the public interest or in the exercise of official authority; or (f) necessary for the *data controller's* or recipient's legitimate interests, except where overridden by the interests of the *data subject*. The general principles of data processing are that personal data is: (a) processed fairly and lawfully; (b) collected for specific, explicit and legitimate purposes and not processed in a manner incompatible with those purposes; (c) adequate, relevant and not excessive; (d) accurate and, where necessary, up to date; (e) kept in an identifiable form for no longer than necessary (Articles 6 and 7, *Data Protection Directive*).

standard conditions for processing sensitive personal data	means the processing: (a) is carried out with the *data subject's* explicit consent; or (b) is necessary for a legal obligation in the field of employment law; or (c) is necessary to protect the vital interests of the *data subject* where the *data subject* is unable to give consent; or (d) is carried out by a non-profit-seeking body and relates to members of that body or persons who have regular contact; or (e) relates to data made public by the *data subject*; or (f) is necessary for legal claims; or (g) is necessary for medical reasons (Article 8(2) and 8(3), *Data Protection Directive*).
standard conditions for transborder dataflow	means the *transborder dataflow*: (a) is to a *whitelisted country*; (b) is made pursuant to a set of *Model Contracts*; (c) is made pursuant to *binding corporate rules* (if permitted in that jurisdiction); (d) is made with the *data subject's* consent; or (e) is necessary for the performance of a contract with, or in the interests of, the *data subject*; (f) is necessary or legally required on important public interest grounds, or for legal claims; or (g) is necessary to protect the vital interests of the *data subject*; or (f) is made from a public register (Article 25 and 26, *Data Protection Directive*).
standard definition of 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 identity (Article 2(a), *Data Protection Directive*)
standard types of sensitive personal data	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life (Article 8, *Data Protection Directive*).
standard processor obligations	means obligations on the *data processor* to only act on instructions from the *data controller* and to comply with the *general security obligations* (Article 17, *Data Protection Directive*).
standard territorial test	means the application of a state's national law to the processing of personal data by a *data controller* : (a) in the context of an establishment in the territory of that state; (b) not established in the territory of that state, but in a place where its national law applies by virtue of international public law; (c) using of equipment in that state (other than for transit) where that *data controller* is not established on Community territory.
subject access information	means the provision of: (a) confirmation as to whether data relating to a *data subject* are being processed and information as to the purposes of the processing, the categories of data, and the recipients to whom the data are disclosed; (b) communication of the data undergoing processing and of any available information as to their source; and (c) knowledge of the logic involved in any automatic processing of data concerning the *data subject* (Article 12, *Data Protection Directive*).
transborder dataflows	means: (a) in the case of an EEA State, the transfer of personal data from a destination within the EEA to a destination outside of the EEA; and (b) in the case of other States, a transfer of personal data from within that State to any another State.
whitelisted country	means countries that the Commission has found to provide an adequate level of protection for personal data. This currently comprises Andorra, Argentina, Canada (partially), the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, Switzerland and organisations in the US which have committed themselves to the "Safe Harbor".

Contacts.

Argentina

Pablo Andrés Palazzi
Allende & Brea
Tel: + 5411 4318 9900
pap@allendebrea.com.ar
www.allendebrea.com.ar

Australia

Michael Pattison
Allens
Tel: +61 3 9613 8839
michael.pattison@allens.com.au
www.allens.com.au

Gavin Smith
Allens
Tel: +61 2 9230 4891
gavin.smith@aar.com.au
www.allens.com.au

Austria

Christian Schmelz
Günther Leissler
Schönherr Rechtsanwälte GmbH Attorneys at Law
Tel: (43) 1 534 37 227
c.schmelz@schoenherr.at
g.leissler@schoenerr.at
www.schoenherr.at

Belgium

Tanguy Van Overstraeten
Linklaters LLP
Tel: (32) 2 501 94 05
tvanover@linklaters.com
www.linklaters.be

Brazil

Mariá Guitti
Lefosse Advogados
Tel: (55) 11 3024 6220
maria.guitti@linklaters.com
www.lefosse.com.br

Bulgaria

Zdravka M. Ugrinova
Djingov, Gouginski, Kyutchukov & Velichkov
Tel: (359) 2 932 1100
zdravka.ugrinova@dgkv.com
www.dgkv.com

Canada

Charles Morgan
McCarthy Tétrault LLP
Tel: (1) 514-397-4230
cmorgan@mccarthy.ca
www.mccarthy.ca

Cyprus

Ms Galatia Sazeidou
Georgiades & Pelides LLC
Tel: (357) 22 88 9000
gsazeidou@cypruslaw.com.cy
www.cypruslaw.com.cy

Czech Republic

Barbora Ležatková
Hana Gawlasová
Kinstellar, s.r.o., advokátní kancelář
Tel: (420) 221 622 224/125
barbora.lezatkova@kinstellar.com
hana.gawlasova@kinstellar.com
www.kinstellar.com

Denmark

Jakob Skaadstrup Andersen
Gorrissen Federspiel
Tel: (45) 33 41 41 41
jsa@gorrissenfederspiel.com
www.gorrissenfederspiel.com

DIFC

Scott Campbell
Linklaters LLP
Tel: (971) 4 369 5800
scott.campbell@linklaters.com
www.linklaters.com

Estonia

Ants Nõmper
Raidla Lejins & Norcous
Tel: (372) 6 407 170
ants.nomper@rln.ee
www.rln.ee

Finland

Kaisa Fahllund
Erkko Korhonen
Hannes Snellman Attorneys Ltd
Tel: (358) 9 228 841
kaisa.fahllund@hannessnellman.com
www.hannessnellman.com

France

Sylvie Rousseau
Linklaters LLP
Tel: (33) 1 56 43 27 08
sylvie.rousseau@linklaters.com
www.linklaters.com

Germany

Dr Daniel Pauly
Linklaters LLP
Tel: (49) 69 71003-570
daniel.pauly@linklaters.com
www.linklaters.com

Dr Konrad Berger
Linklaters LLP
Tel: (49) 89 4 18 08 0
konrad.berger@linklaters.com
www.linklaters.com

Greece

Maria Giannakaki
Karageorgiou & Associates Law Firm
Tel: (30) 210 7221021
giannakaki.m@dsa.gr
www.kalaw.gr

Hong Kong

Rowan McKenzie
Deborah Papworth
Adrian Fisher
Linklaters LLP
Tel: +852 2842 4110
rowan.mckenzie@linklaters.com
deborah.papworth@linklaters.co
adrian.fisher@linklaters.com
www.linklaters.com

Hungary

Dr. Dávid Klacsmann
Andrékó Kinstellar Ügyvédi Iroda, Budapest
Switchboard: +36 1 428 4400
david.klacsmann@kinstellar.com
www.kinstellar.com

Iceland

Hjördís Halldórsdóttir
Áslaug Björgvinsdóttir
LOGOS - Legal Services
Tel: (354) 5 400 300
hjordis@logos.is
aslaug@logos.is
www.logos.is

Indonesia

David Holme
Widyawan & Partners
Tel: +62 21 2995 1500
davidholme@widawanpartners.com
www.wnplaw.com

India

Praveen Thomas
Talwar Thakore & Associates
Tel: (91) 22 6613 6942
praveen.thomas@tta.in

Ireland

Philip Nolan
Mason Hayes + Curran
Tel: (353) 1 614 5000
pnolan@mhc.ie
www.mhc.ie

Israel

Omer Tene
Tene & Associates
Tel: (972) 504 770 218
omer.tene@bezeqint.net
www.omertene.com

Italy

Avv. Daniele Vecchi
Avv. Melissa Marchese
Gianni, Origoni, Grippo & Partners
Tel: (39) 02 763741
dvecchi@gop.it
mmarchese@gop.it
www.gop.it

Japan

Stephen Webb
Mamiko Nagai
Linklaters Tokyo
Tel: (81) 3 6212 1249
(81) 3 6212 1232
stephen.webb@linklaters.com
mamiko.nagai@linklaters.com
www.linklaters.com

Latvia

Sarmis Spilbergs
LAWIN
Tel: (371) 781 4848
sarmis.spilberg@lawin.lv
www.lawin.lv

Liechtenstein

Odile Fillacier
Markus Wanger
Wanger Advokaturbüro
Tel: (423) 237 52 52
odile.fillacier@wanger.net
markus.wanger@wanger.net
www.wanger.net

Lithuania

Dr. Jaunius Gumbis
Lideika, Petrauskas, Valiunas ir partneriai
LAWIN
Tel: (370) 5 268 1830
jaunius.gumbis@lawin.lt
www.lawin.lt

Luxembourg

Olivier Reisch
Linklaters LLP
Tel: (352) 26 08 1
olivier.reisch@linklaters.com
www.linklaters.com

Malta

Dr Brigitte Zammit
Emirates International Telecommunications LLC
Tel: (971) 4 433 10 40
brigitte.zammit@eitl.ae
www.eitl.ae

Andrew Muscat
Mamo TCV Advocates
Tel: (356) 2123 1345 or
(356) 2123 2271
andrew.muscat@mamotcv.com
www.mamotcv.com

Mexico

Pablo Perezalonso Eguía
Ritch Mueller, S.C.
Tel: (5255) 9178 7050
pperezalonso@ritch.com.mx
www.ritch.com.mx

The Netherlands

Paul Kreijger
Vincent Gerlach
Linklaters LLP
Tel: (31) 20 799 6200
paul.kreijger@linklaters.com
vincent.gerlach@linklaters.com
www.linklaters.com

Norway

Rune Opdahl
Advokatfirmaet Wiersholm AS
Tel: (47) 210 210 00
rop@wiershold.no
www.wiersholm.no

PRC

Adrian Fisher
Zhirong Zhou
Linklaters LLP
Tel: (86 21) 2891 1888
adrian.fisher@linklaters.com
shirong.zhou@linklaters.com
www.linklaters.com

Poland

Ewa Kurowska-Tober
Linklaters, C.Wiśniewski i Wspólnicy Spółka Komandytowa
Tel: (48) 22 526 50 46
ewa.kurowska-tober@linklaters.com
www.linklaters.com

Portugal

Carlos Pinto Correia
Linklaters LLP
Tel: (351) 21 864 00 32
carlos.correia@linklaters.com
www.linklaters.com

Romania

Oana Radulescu
Oana Costache
Kinstellar
Tel: 40 (0) 21 307 1624/1620
oana.radulescu@kinstellar.com
oana.costache@kinstellar.com
www.kinstellar.com

Russia

Galina Tereschenko
Linklaters CIS
Tel: (7 495) 797 9797
galina.tereschenko@linklaters.com
www.linklaters.com

Singapore

Sophie Mathur
Laure de Panafieu
Adrian Fisher
Linklaters Singapore Pte. Ltd.
Tel: +(65) 6692 5700
sophie.mathur@linklaters.com
laure.de_panafieu@Linklaters.com
adrian.fisher@linklaters.com
www.linklates.com

Slovakia

Zuzana Turayová
Kinstellar, s.r.o.
Tel: (421) 2 5929 1148
zuzana.turayova@kinstellar.com
www.kinstellar.com

Slovenia

Dr Matthias Wahl
Sorsak Jani
Schönherr Rechtsanwälte GmbH
Tel: (386) 12000 980
m.wahl@schoenherr.at
j.sorsak@schoenherr.eu
www.schoenherr.at

Spain

Carmen Burgos
Linklaters S.L.P
Tel: (34) 91 399 60 88
carmen.burgos@linklaters.com
www.linklaters.com

Sweden

Emma Linnér
Linklaters Advokatbyrå AB
Tel: (46) 8 665 66 93
emma.linner@linklaters.com
www.linklaters.com

Switzerland

David Rosenthal
Homburger AG
Tel: (41) 43 222 10 00
david.rosenthal@homburger.ch
www.homburger.ch

Ukraine

Oleh Malskyy
Yulia Yanyuk
AstapovLawyers International Law Group
Tel: +38 (044) 490 70 01
malskyy@astapovlawyers.com
yanyuk@astapovlawyers.com
www.astapovlawyers.com

United Kingdom

Marly Didizian
Richard Cumbley
Linklaters LLP
Tel: (44) 20 7456 2000
marly.didizian@linklaters.com
richard.cumbley@linklaters.com
www.linklaters.com

Vietnam

Bill Magennis
Vinh Dang
Ngoc Anh Tran
Allens
Tel: (84)903 404 440
bill.magennis@allens.com
vinh.dang@allens.com
ngocanh.tran@allens.com
www.allens.com

General Editor: Peter Church, Linklaters LLP, London

Assistant Editors: Megan Page and Richard Liversidge, Linklaters LLP, London

Linklaters LLP, One Silk Street, London EC2Y 8HQ. Tel: (44) 20 7456 2000 Fax: (44) 20 7456 2222. www.linklaters.com