Data Protection & Privacy

Jurisdictional comparisons **First edition 2012**

General Editor:
Monika Kuschewsky Van Bael & Bellis

THOMSON REUTERS

General Editor
Monika Kuschewsky
Van Bael & Bellis

Commercial Director
Katie Burrington

Publishing Manager
Emily Kyriacou

Senior Editors
Lisa Naylor

Sub Editor
Caroline Pearce

Design and Production
Dawn McGovern

Published in 2011 by Sweet & Maxwell,
100 Avenue Road, London NW3 3PF
part of Thomson Reuters (Professional) UK Limited
(Registered in England & Wales, Company No 1679046.
Registered Office and address for service:
Aldgate House, 33 Aldgate High Street, London EC3N 1DL)

A CIP catalogue record for this book is available from the British Library.

ISBN: 978-1-908239-14-3

Contents

Preface Monika Kuschewsky Van Bael & Bellis v

Foreword Viviane Reding, Vice-President of the European Commission, Commissioner for Justice, Fundamental Rights and Citizenship vii

Foreword Peter Hustinx, European Data Protection Supervisor xi

Foreword Jean Gonié, Director of Privacy, EU Affairs, Microsoft Europe xiii

Austria Dr Rainer Knyrim Preslmayr Rechtsanwälte OG 1

Belgium Monika Kuschewsky Van Bael & Bellis 23

Canada Sean Lind & David Elder Stikeman Elliott 43

Cyprus Nicholas Ktenas & Chrystalla Neophytou Andreas Neocleous & Co LLC 69

Czech Republic Richard Otevrel Havel, Holásek & Partners 89

Denmark Johnny Petersen Delacour Dania 109

EU Monika Kuschewsky Van Bael & Bellis 131

France Raphaël Dana & Ramiro Tavella Sarrut Avocats 151

Germany Monika Kuschewsky Van Bael & Bellis 171

Hungary Janos Tamas Varga VJT & Partners 199

India Naheed T Carrimjee Desai Desai Carrimjee & Mulla 223

Israel Yoheved Novogroder-Shoshan Yigal Arnon & Co 239

Italy Gerolamo Pellicanò & Giovanna Boschetti CBA Studio Legale e Tributario 263

Latvia Linda Lejina, Ilze Bukaldere Attorneys at Law Borenius 289

Luxembourg Héloïse Bock Arendt & Medernach 317

Malta Michael Zammit Maempel & Mark Hyzler GVTH Advocates 337

Mexico Laura Collada & Jorge Molet Dumont Bergman Bider & Co., S.C. 357

Netherlands Polo van der Putt & Eva de Vries Vondst Advocaten 377

Poland Agata Szeliga Sołtysinski, Kawecki & Szlezak 397

Portugal Mónica Oliveira Costa Coelho Ribeiro e Associados 423

Republic of Ireland Jeanne Kelly & Aoife Treacy Mason, Hayes & Curran 445

Romania Roxana Ionescu & Ovidiu Balaceanu Nestor Nestor Diculescu Kingston Petersen 467

Slovakia Richard Otevrel & Jaroslav Šuchman Havel, Holásek & Partners 495

South Africa André Visser & Danie Strachan Adams & Adams 519

Spain Cecilia Álvarez Rigaudias & Leticia López-Lapuente Uría Menéndez 539

Sweden Erica Wiking Häger, Mikael Moreira & Anna Nidén Mannheimer Swartling 563

Switzerland Lukas Morscher Lenz & Staehelin 587

Turkey Gönenç Gürkaynak, Ilay Yılmaz & Ceren Yıldız ELIG Attorneys at Law 607
UK Hazel Grant & Mark Watts Bristows 615
USA Andrew B Serwin Foley & Lardner 637
Contacts

Preface

Monika Kuschewsky Partner and Head of the European Data Protection Practice, Van Bael & Bellis

Processing of individuals' data is an essential part of modern business. Whether they are selling goods or services, businesses are processing information regarding their employees, customers, consumers and suppliers in ever-increasing volumes. The advent of high-speed internet, web-connected mobile devices and user-generated content means that the collection, exchange and analysis of data has never been easier, faster or more valuable. New technologies and services, such as cloud computing, online behavioural advertising and geolocation services, are all required to respect the applicable data protection laws.

As technology is advancing, so are regulators. Countries across the globe have recognised the importance of protecting individuals' data and they are responding accordingly with increasingly energetic legislative and related efforts: the OECD with its review of the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data; the Council of Europe with its revision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); the European Commission with its proposal for a new European data protection framework; and the APEC with the Honolulu Declaration, by virtue of which APEC member countries agreed to implement the APEC Cross-Border Privacy Rules System, to mention just a few examples. Administrative and criminal proceedings imposing heavy fines and even imprisonment, as well as civil damages claims, are on the rise. A key concern for businesses in particular is that bad publicity from data protection violations can seriously damage goodwill, brand image and consumer trust. A business' data processing activities can be a major asset or a major liability, the difference depending on its ability to manage the legal risks associated with data processing.

These risks are not only present at national level. As globalisation continues, businesses are processing data from countries all around the world. As a result, they need to keep up with a field of law which is developing quickly in a wide array of jurisdictions.

Data Protection & Privacy – Jurisdictional Comparisons provides companies, legal professionals and data protection officers with an essential reference guide and key information on data protection and privacy laws in more than 30 major jurisdictions worldwide. Written by leading local practitioners who are experts in the field of data protection and privacy, each chapter covers a different national jurisdiction and highlights all of the major aspects of data protection within that jurisdiction. Each chapter answers pertinent questions regarding legislation (current and pending), data protection authorities, the legal basis for data processing, information obligations, rights of individuals, registration obligations, data protection officers, international data transfers,

security of data processing and enforcement, sanctions, remedies and liability.

The reader-friendly Q&A format, used successfully in other volumes of *The European Lawyer Reference Series*, allows for easy cross-jurisdictional comparisons, providing a single starting point of reference. While by no means a substitute to seeking the advice of local counsel, this book facilitates understanding of the diversity of legislation and compliance with data protection frameworks in the global context.

Brussels, December 2011

The origins of data protection law

Vice-President Viviane Reding Member of the European Commission responsible for Justice, Fundamental Rights and Citizenship

Data protection legislation has developed in parallel with information technology. In the 1970s, when the first computers were installed in public administrations and businesses for the processing of huge amounts of data, it became clear that the new technology also had potential to exercise control over citizens through the processing of their personal data.

At that time, dictatorial regimes still controlled large parts of Europe, and the memory of recent dictatorships was still fresh in the democratic countries. There was a clear understanding that safeguards had to be created to prevent the misuse of personal data. The USA and several European countries adopted the first data protection and privacy laws. While lawmakers focused on protecting the freedom of citizens against inappropriate interventions by state authorities, it was already clear at the time that big economic players were also in a position to exercise considerable power over individuals about whom they had huge amounts of data. Many data protection laws address this issue and apply the same principles to private and public entities alike.

From the very beginning of data protection legislation, the cross-border transfer of data was a matter for particular concern. Legislators were well aware that nothing could be exported as easily as data and moved out of the jurisdiction where national law could ensure proper protection and supervision. Lawmakers therefore introduced specific safeguards and procedures for cross-border transfers of data. With the advancement of data processing, closer economic integration and the emergence of global businesses, there was an increasing need to reconcile global commerce and data protection. Organisations such as the Organisation for Economic Cooperation and Development, the Council of Europe and the European Communities began to define data protection principles at international level and to foster agreements that would allow the transfer of data on the basis of these common standards. The adoption of the European Data Protection Directive in 1995 marked the creation of the world's largest area of free flow of personal data on the basis of commonly agreed safeguards for the protection of citizens' privacy rights. With the enlargement of the EU, this area now comprises more than 500 million citizens and produces more than a quarter of the world's gross domestic product (according to IMF 2010 statistics).

Growing diversity

The European approach to data processing is based on a set of common rules for data protection which are applied to all processing of personal data, whether in the private or the public sector. For historical reasons, specific rules apply to police and judicial cooperation in criminal matters, an area that was not covered by the same legal basis as other EC competences until the entry into force of the Lisbon Treaty. For the EU Single Market, the same data protection rules apply to all sectors, with the exception of the electronic communications sector, where legislators recognised the specific sensitivity of communications and location-based data. Therefore, specific rules apply in the communications sector to address the potential risk to citizens' fundamental rights.

In other jurisdictions, such as the USA, legislators adopted privacy legislation for specific sectors of the economy: eg financial services, health, entertainment or marketing services. Some EU member states have reacted to public demand and have introduced national rules covering specific areas in addition to the EU framework. Legislation at state level in the US or at regional level in EU member states further adds to the legal diversity in this area.

Diversity of legislation and administrative requirements constitute obstacles for international businesses when they have to comply with different rules in different jurisdictions which may even be contradictory. Globalisation, economic integration and technical progress are international processes by default. As a result, businesses may increasingly find themselves in violation of laws in some countries. Businesses could not only face litigation or prosecution, but also endanger their reputation. If the public perceives businesses as not taking the protection of personal data seriously, this may have implications well beyond the reputation of the companies concerned. The confidence of citizens in the online economy as a whole could be undermined. Public opinion surveys, such as the Eurobarometer, already show an increasing scepticism by EU citizens in respect of their online privacy. We have to regain this trust so that citizens take up new services and fully benefit from the economic and social gains that new technologies and business ideas provide.

The need for reform

Most of the principles of data protection have stood the test of time. However, we need to clarify them and make their practical application easier and more effective. The Lisbon Treaty provides a new legal basis for data protection reform, which will simplify and harmonise legal requirements in the EU and create a level playing field for businesses. At the same time, it will increase transparency and make it easier for individuals to exercise their data protection rights effectively.

The challenge of how best to protect citizens' rights and at the same time facilitate legitimate data processing for businesses is not limited to the EU. Public debate on the protection of privacy and personal data is ongoing in many countries around the globe. There is broad agreement on the

basic principles between democratic countries and we should continue the international dialogue to find practical arrangements for our citizens in a globalised economy.

This book, with its overview of existing data protection requirements in the world's most important economies, comes at a crucial moment and can serve as a reference in the forthcoming discussions on the future of data protection at global, regional and national levels.

The Treaty of Lisbon requires the EU legislator to lay down a comprehensive set of data protection rules that apply to all fields of EU competence, including law enforcement and justice. Establishing rules for this area that ensure appropriate protection of personal data is not only relevant to the public sector. As personal data from private entities are increasingly accessed by law enforcement and security services, this aspect needs to be looked at more closely. This is particularly relevant in cases where the data may be accessed by public authorities outside the jurisdiction of the user. Direct negotiations and bilateral agreements, based on a common commitment to the need for a high level of data protection in a free and democratic society, are the way forward to ensure that personal data are safe, both inside and outside the EU.

The European Commission is committed to using all means at its disposal to ensure that the fundamental rights of individuals are respected, both within the EU and in exchanges with our international partners.

Brussels, December 2011

Foreword

Peter Hustinx European Data Protection Supervisor

I warmly welcome the initiative of *The European Lawyer Reference Series* to publish this cross-border Data Protection and Privacy book, reflecting the state of play on data protection and privacy in more than 30 major jurisdictions around the world. Therefore, I have also gladly accepted their invitation to provide a brief foreword. Let me just highlight three relevant dimensions of this publication.

First of all, this book clearly illustrates how far the concept of data protection has now spread around the world. What was conceived in a few, mainly European, jurisdictions in order to protect individuals in view of the increasing use of information technology in a wide variety of fields, long before the development of the internet into its present reality, has now become a subject of professional legal attention and action in many countries around the world. The number of jurisdictions with some data protection law on record would probably easily exceed twice the number of those covered in this book, but there can be no doubt that those covered here are among the most relevant, in any case for the use of legal professionals specialised in this field. In the meantime, the state of the law on data protection in Europe has also developed and diversified. The protection of personal data has been explicitly recognised as a fundamental right in the Charter of Fundamental Rights of the European Union and a substantial body of European and national laws and jurisprudence has developed to give legal effect to this right. Similar conclusions emerge from the contributions on other jurisdictions covered in this book.

Secondly, this book also illustrates that legal concepts and principles alone will never succeed in reaching their goals if they are not also applied in practice. In this case, let me emphasise that legal practice will be important but not sufficient. Data protection is designed to be applied in the daily practice of information systems and where the rights and interests of the individuals concerned are at stake. However, legal practice can be of immense help in driving this process forward. It is in this spirit that I hope this book will be very useful for legal professionals who need information about the state of the law outside their own jurisdiction. Cross-border issues will increasingly require cross-border thinking. This will be more important than ever before, where information infrastructures will increasingly allow data to be 'in the cloud' or 'everywhere' and where data already move globally overnight on a daily basis for a host of largely legitimate reasons. It is therefore crucial that we continue to invest in the quality of our current data protection laws in order to ensure that they continue to be sufficiently effective in the highly dynamic environments of today and tomorrow.

This brings me to the third dimension of this book: it reflects the current state of play in various jurisdictions, but in doing so it also highlights the

need for review and further development. Such a major review is ongoing in the European Union with a view to meeting the challenges of new technologies and globalisation, and this review coincides with similar exercises in the Council of Europe and the Organisation for Economic Cooperation and Development, all aimed at ensuring that our present legal frameworks continue to be fully effective in the future. As to the EU, this will no doubt result in a strengthening of key roles: more effective rights for data subjects; more effective accountability for data controllers; more effective enforcement by data protection authorities; and more effective cross-border cooperation. There is of course more to be said about this, but the key messages will be simple: it will be about delivering fundamental values in practice, in a more global and technological environment.

I trust that this book will be a very useful guide for legal professionals and will also contribute to further reflection on how to make data protection more effective in 2015 and beyond.

Brussels, December 2011

Foreword

Jean Gonié Director of Privacy, EU Affairs, Microsoft

From Budapest to Washington DC, from Jerusalem to Delhi, data travel all over the world, and legal issues travel with them.

For a worldwide company like Microsoft, with global presence and visibility, this requires a high degree of responsibility to ensure that we are doing the right things. It is essential for us to provide clear and easy-to-understand information on our privacy practices and to respond adequately to questions about location and access to data, and about the way data are collected and used.

We operate in an environment where expectations are high and regulations are stringent and not harmonised. Indeed, data protection regimes differ from country to country and in order to be compliant, global companies in particular need to have a clear and comprehensive understanding of the legal landscape on a worldwide level. For example, Microsoft's Hotmail email service, with its 350 million active accounts around the world operates out of data centres in the US, EU and other places, and is therefore subject to the legal regimes of multiple jurisdictions.

This is also a challenge in light of the development of cloud computing, since not only cloud service providers, but also their subcontractors and customers must have assurances as to how the law will affect the storage, processing and use of data.

Trying to understand the way the current patchwork of national and regional laws around the world applies is, of course, a priority for the legal ecosystem. But not every size of company can do so easily because they lack resources.

To address these challenges, a global organisation – like any other company – needs certainty and greater clarity, including about which law or laws apply to the processing of data and what the requirements are.

That is why this book, written by leading privacy law experts providing a reference point for the data protection laws of more than 30 jurisdictions worldwide, should respond to many questions and solve a lot of issues by facilitating the understanding of the application of the law, increasing legal certainty and eventually making the future more predictable.

I am convinced that this book will soon become the new *vade mecum* for the current and next generation of privacy and data protection professionals.

Brussels, December 2011

Austria

Preslmayr Rechtsanwälte OG Dr Rainer Knyrim

1. LEGISLATION

1.1 Name/title of the law

The Austrian Data Protection Act (ADPA), enacted in 2000, implementing the EU Data Protection Directive 95/46/EC (the Directive), regulates which personal data might be processed by whom and under what circumstances and conditions. It is the general legal framework for data protection in Austria.

Besides the ADPA, privacy-related provisions can be found, for example, in the Telecommunications Act regarding electronic advertising, in the Act on Banking regarding the banking secrecy as well as in the Labour Constitutional Act regarding data applications for personnel administration and evaluation.

1.2 Pending legislation

The Data Protection Act was recently amended in 2010. The main focus of this amendment was the introduction of rules on video surveillance and a data breach notification obligation. Thus, there are no major amendments expected in the near future apart from the introduction of an obligatory online filing procedure for notifications of data applications with the Austrian data protection authority at the end of September 2012.

Amendments to the ePrivacy Directive will mainly be implemented through changes to the Telecommunications Act. The implementation of Article 5(3) of the Directive will be effected by new wording for section 96(3) Telecommunications Act. It stipulates that operatives of communication services are obliged to inform the participant or the user about the processing or transferring of any personal data. In addition, the legal grounds and the purpose for data processing have to be mentioned too. Data collection is only permitted if the participant or user has given his/her consent to it.

Article 6 of the Directive will be implemented in section 99 Telecommunications Act. Section 99(1) stipulates that traffic data are in general not to be stored and that they have to be deleted or anonymised after ending the connection.

Another amendment will be implemented in section 102 Telecommunications Act. These amendments are already agreed upon with the national assembly but the new wording has not been published in the Federal Law Gazette yet.

1.3 Scope of the law

1.3.1 The main players

- The 'data subject' is any natural or legal person or group of natural persons

not identical to the data controller, whose personal data are processed.

- The 'data controller' is a natural or legal person, group of persons or organ of a territorial corporate body (or respectively the offices of such organs), who decides alone or jointly with others the purposes of any processing of personal data whether it is processing data themselves or has it done by somebody else (data processor). Qualification as a data controller remains, if the commissioned data processor decides himself to process data for a specific purpose, unless this was expressly prohibited or the data processor has to decide on its own due to legal provisions or professional rules regarding the processing of data.
- The 'data processor' is any natural or legal person, group of persons or organ of a territorial corporate body (or respectively the offices of such organs), if they use data only for a commissioned work.

1.3.2 Types of data

The ADPA covers personal data relating to natural persons and data relating to legal persons (eg companies).

'Personal data' are defined as information relating to data subjects which are identified or identifiable; data are only 'indirectly personal' for a data controller, a data processor or a recipient of a transmission if the data, indeed, relate to the data subject but do not allow the data controller, data processor or recipient of a transmission to identity the data subject by legal means.

'Sensitive data' are data relating to natural persons concerning their racial or ethnic origin, political opinion, trade union membership, religious or philosophical beliefs and data concerning health or sex life.

Personal data which have been anonymised by removing the link to the person are not considered to be personal data, provided that the anonymisation is absolute and cannot be reversed by any reasonable means likely to be used. If personal data can be linked to an identified or identifiable person by means of a code, the data will be considered to be personal data.

1.3.3 Types of acts/operations

The ADPA covers the processing of personal data, which is defined as any kind of operation with or use of the data, including: the collection; the storage; the sequencing; the comparing; the amending; the linking; the copying; the polling; the use; the transfer to a data processor; the locking; or any other operation of data.

In general only automatic data processing is covered. But there is one exception stipulated in section 58 ADPA. If structured manual data sets exist for the purpose of business affairs where the Federation has the power to pass laws, they are deemed to be data applications according to section 4(7). Section 17 shall apply insofar as the obligation to notify applies only to those data sets whose content is subject to prior checking. A 'data application' is the sum of logically linked stages of data use, which are organised in order to reach a defined result and which are as a whole or partially performed automatically, that is, performed by machines and controlled through programs (automated data processing).

1.3.4 Exceptions

The processing of personal data by a natural person in the course of a purely personal or family matter falls outside the scope of the ADPA if the data have been disclosed by the data subject himself or if they were received lawfully.

1.3.5 Geographical scope of application

The ADPA applies to the use of personal data in Austria. The ADPA also applies to the use of data outside of Austria, insofar as the data are used in other member states of the European Union for the purposes of the main establishment or a branch establishment of the data controller in Austria. However, deviating from this general rule, the law of the state where the data controller has its seat applies, where a data controller in the private sector whose seat is in another member state of the European Union uses personal data in Austria for a purpose that cannot be ascribed to any of the data controller's establishments in Austria. Furthermore, said law shall not be applied insofar as the data are only transmitted through Austrian territory.

1.4 Particularities

The ADPA also protects personal data relating to legal persons such as companies.

Joint Information System

Another form of data processing is the 'joint information system'. According to section 4(13) ADPA, a joint information system is the following: joint processing of personal data in a data application by several data controllers and the joint utilisation of the data so that every data controller has access even to those data in the system that have been made available to the system by other data controllers.

It is interesting that although the Directive did not mention joint information systems, the Austrian legislative authority had the opinion that these systems deserve special attention. Joint information systems are subject to prior checking according to section 18 ADPA and in most cases the Data Protection Authority requires consent or at least that all data subjects included in this system are informed of the processing of their data.

2. DATA PROTECTION AUTHORITY

Name: Data Protection Authority (*Datenschutzkommission*)
Address: Hohenstaufengasse 3, 1010 Vienna, Austria
T: +43 (0) 1 531 15 2525
F: +43 (0) 1 531 15 2690
E: dsk@dsk.gv.at
W: *www.dsk.gv.at*

2.1 Role and tasks

The Data Protection Authority (DPA) is an independent body and ensures that individual rights and interests in secrecy deserving protection are

protected. Another responsibility of the DPA is to handle complaints (Ombudsman).

2.2 Powers

The DPA decides on notifications of data applications, applications for authorisations of data transfers to countries outside the European Economic Area (EEA) if they do not provide an adequate level of protection and functions as a complaint authority for anyone whose rights for privacy or data protection have (allegedly) been infringed.

2.3 Priorities

The priorities of the DPA mainly relate to treating the notifications of data applications and the applications for authorisation of international data transfers. Furthermore, the DPA deals with the amendments to the ADPA, re amending or implementing new regulations or new instruments of the ADPA such as have been introduced by the recent amendment in 2010 (regulations on video surveillance and the data breach notification duty).

The Data Protection Authority publishes a report about its activities at least every two years according to section 38(4) ADPA. This report shall be forwarded to the Federal Chancellor. The report contains information about the work done the last two years but usually does not give an outlook on future priorities.

3. LEGAL BASIS FOR DATA PROCESSING

According to the ADPA, personal data shall only be used fairly and lawfully, shall only be collected for specific, explicit and legitimate purposes and shall be used insofar as they are essential for the purpose of the data application. In addition, personal data shall be processed only insofar as the purpose and content of the data application are covered by the statutory competencies or the legitimate authority of the respective data controller and the data subject's interest in secrecy deserving protection is not infringed.

3.1 Consent

3.1.1 Definition

'Consent' is the valid declaration of intention by the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances.

3.1.2 Form

In principle, it is not required to obtain consent in writing. For the sake of evidence it is recommended to require written consent, though; however, writing does not mean handwritten, consent can also be given, for example, via email.

3.1.3 In an employment relationship

Consent must be given unambiguously and freely. Valid consent is a

legitimate ground for data processing, but the DPA tends to doubt that employee consent is given freely.

3.2 Other legal grounds for data processing

Non-sensitive personal data may be processed if one of the following conditions is met:

- an explicit legal authorisation or obligation to use the data exists; or
- the data subject has given his consent, which can be revoked at any time, the revocation rendering any further use of the data illegal; or
- vital interests of the data subject require the use; or
- overriding interests pursued by the data controller or by a third party require the use of the data.

The use of legitimately published data and merely indirectly personal data shall not constitute an infringement of interests in secrecy deserving protection. The right to object to the use of such data remains unaffected.

If sensitive data are processed, the secrecy deserving protection is not infringed if:

- the data subject has obviously made public the data himself;
- the data are used only in indirect personal form;
- the obligation or authorisation to use the data is stipulated by law, in so far as it serves an important public interest, or is used by a data controller in the public sector to fulfil his obligation to give assistance to the authorities;
- data are used that solely concern the exercise of a public office by the data subject;
- the data subject has unambiguously given his consent, which can be revoked at any time, the revocation rendering any further use of the data illegal;
- the processing or transmission is in the vital interest of the data subject and his consent cannot be obtained in time;
- the use is in the vital interest of a third party;
- the use is necessary for the establishment, exercise or defence of legal claims by the data controller before a public authority and the data were collected legitimately;
- the data are used for private purposes;
- the use is required according to the rights and duties of the data controller in the field of employment law and civil service regulations and is legitimate according to specific legal provisions – the rights of the labour councils according to the Labour Constitution Act (*ArbVG*) with regard to the use of data remain unaffected;
- the data are required for the purpose of preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health care services and the use of data is performed by a medical person or other person subject to an equivalent duty of secrecy; or
- non profit organisations with a political, philosophical, religious or trade union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities,

as long as these are data of members, sponsors or other persons who display an interest in the aim of the organisation on a regular basis - these data shall not be disclosed to a third party without the consent of the data subject unless otherwise provided for by law.

As regards the employment relationship, employee privacy laws and regulations require – as a general principle of Austrian privacy and data protection law – that personal data of employees are only processed to the extent that they are absolutely necessary for the given purpose. Furthermore, those regulations require the employer as the data controller to effectively inform the employees about the personal data processed as well as about any alterations or amendments to any data application and processing of personal data. Where a works council is established, the employees' interests regarding privacy are represented by this body. Either the works council has to be informed about any data applications using personal data of the employees (transfers to data processors included) or prior consent of the works council to any measures having a massive impact on the employee's privacy is required.

3.3 Direct marketing and cookies

There are currently no specific regulations in place on these issues. Rather, the general principles and the provisions of the ADPA and the Telecommunications Act apply.

Before the implementation of Article 14 of the Directive there was no separate right to object to data processing in the ADPA. Whereas Article 14 *lit. a*) was implemented with the ADPA, Art 14 *lit b*) was not considered in the ADPA, because it was already implemented in section 151 of the Industrial Code.

However, in order to implement the amendments to the ePrivacy Directive 2002/58/EC brought about by Directive 2009/136/EG, the Telecommunications Act will have to be amended. Drafts of the amendment are already available and entry into force of the amendment is expected in 2012.

New rules under the Directive provide increased opportunities for the legitimate use of cookies which contain personal data. As already mentioned above, the Directive will be implemented through amendments to the Telecommunications Act.

Approval or consent from the data subject is required and must be given on the basis of clear and comprehensive information.

3.4 Data quality requirements

In Austria, there are requirements as to the quality of personal data to be processed. The following quality principles have to be respected:

- fairness and legality;
- purpose limitation principle;
- limitation on the amount of data;
- correctness and actuality; and
- time limits.

3.5 Outsourcing

Data controllers may contract with data processors for their data applications insofar as the latter sufficiently warrant the legitimate and secure use of personal data. The data controller shall enter into agreements with the data processor in accordance with the ADPA and check that the agreements are complied with by acquiring the necessary information about the actual data protection and data security measures implemented by the data processor.

If the data controller wants to contract with a data processor in the public sector for a data application subject to prior checking, this has to be notified to the DPA.

Data applications which contain:

- sensitive data; or
- data about offences under section 8(4); or
- whose purpose is to give information on the data subject's creditworthiness; or
- that are carried out in form of a joint information system,

shall be initiated only after an examination (prior checking) by the DPA.

Data applications which are not subject to prior checking only need to meet the requirements of completeness and plausibility. If these requirements are met, the application shall be registered. If the data application contains the information listed above, it is subject to prior checking, which means that the DPA is not able to register the application based on completeness and plausibility. The DPA checks the data application more carefully, eg the legal grounds for transmission, the purpose of the data application and so on.

In addition, data processors have to comply with the following obligations when acting on behalf of a data controller:

- to only use personal data according to the instructions of the data controller – transmission of personal data is prohibited unless instructed by the data controller;
- to take safety measures, in particular by employing staff members who have committed themselves to confidentiality *vis-à-vis* the data processor, or are under a statutory obligation of confidentiality;
- to commission other data processors (subcontractors) only with the permission of the data controller;
- to establish the necessary technical and organisational requirements for the fulfilment of the data controller's obligation to grant the right of information, rectification and erasure, in collaboration with the data controller;
- to hand over all results of the processing and the documentation containing personal data after termination of the processing agreement to the data controller, or destroy the data on request of the data controller; and
- to provide all information to the data controller, which is necessary to ensure the data processor's compliance with the above obligations.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use as well as by means of surveillance cameras is subject to the provisions of the ADPA. For example, consent for the screening of emails is required according to the ADPA.

For video surveillance, the principles of proportionality, purpose limitation and legal processing of data need to be observed.

The provisions on video surveillance are applicable to:

- public places;
- private places (eg, a detached house); and
- private places which may be accessed by the public (eg, a restaurant).

In the course of new provisions in the ADPA, video surveillance may be applied to the protection of life, health and property and for the fulfilment of the legal duty of care.

3.6.2 Employment relationship

The most important regulations requiring the explicit consent of the employee are stated in section 96(1) no 3 of the Labour Constitutional Act (ArbVG), and section 10(1) of the Employment Contracts Adaption Act (AVRAG). Those provisions require consent if the employer wants to introduce, or makes use of, so-called 'employee controlling measures'.

Employee controlling or monitoring measures may include, for example, video surveillance or access control systems (eg a door opener) as well as email and internet monitoring or whistleblowing systems, depending on the particular technical conditions of the system and the intensity of surveillance or control it establishes.

With regard to video surveillance or other monitoring, employees have to be informed and have to give their prior consent to the implementation of the measure via their works council.

This also applies to email monitoring and/or monitoring of internet use. According to section 96(1)(3) of the Labour Relations Act, the employer has to secure the consent of the works council before establishing a monitoring system. Basically, an employee does not have a general right to use email and internet at his/her workplace. But if the use is granted, the employer should establish rules regarding eg the time or frequency of usage which may then be monitored.

In the case of monitoring of business email, it has to be determined how intense the interference is. If the measure exceeds a grade of intensity, the prior consent of the employees and the works committee has to be secured. This also applies to private emailing if this was permitted in the office.

4. INFORMATION OBLIGATIONS

4.1 Who

The data controller has the obligation to inform every single data subject about the processing of his/her personal data.

4.2 What

The information provided has to contain:

- which personal data relating to the data subject are processed;
- the purpose(s) of the data processing;
- the legal grounds for the data processing;
- to whom the personal data are transferred (if a transfer takes place); and
- the name and address of the data controller and of his representatives.

4.3 Exceptions

Information does not have to be provided if the data subject has already been provided with the information about the fact that personal data relating to him are processed. In addition, the information obligation does not apply if:

- the use of the data is provided for by law or an ordinance;
- if it is impossible to provide the information because the data subject cannot be reached; or
- if, considering the improbability of infringement of the data subject's rights and the expenses involved in reaching the data subjects, unreasonable efforts would be required. This applies, in particular, if data are collected for the purposes of scientific research or statistics and the requirement to inform the data subject is not explicitly stipulated. The Federal Chancellor may determine further cases by ordinance in which the duty to provide information does not apply. Until now, such ordinances have not been issued.

In addition, there shall be no duty to provide information regarding data applications that are not subject to notification.

4.4 When

The information should be provided at the time the personal data are recorded.

4.5 How

The data controller has to disclose his identity in an appropriate manner to enable the data subject to assert his/her rights.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The data controller is obliged to provide the data subject with information about the personal data being processed and relating to him, if the data subject requests such information in writing and proves his identity in an appropriate manner.

If no reasons to deny the information exist, the request has to be answered within eight weeks from its receipt.

5.1.2 Exceptions

The information shall not be given insofar as it is essential for the protection of the data subject for special reasons or insofar as overriding legitimate interests pursued by the data controller or by a third party – especially

overriding public interests – are an obstacle to furnishing the information.

Overriding public interests can arise out of the necessity:

- to protect the constitutional institutions of the Republic of Austria;
- to safeguard the operational readiness of the federal army;
- to safeguard the interests of comprehensive national defence;
- to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union; or
- to prevent and prosecute crimes.

The right to refuse to provide the information for the above reasons is subject to control by the DPA.

5.1.3 Deadline

See the answer to section 5.1.1 above.

5.1.4 Charges

The information shall be given free of charge if it concerns the current data files used in a data application and if the data subject has not yet made a request for information to the same controller regarding the same application in the current year. In all other cases a flat rate compensation of EUR 18.89 may be charged; deviations are permitted to cover higher expenses actually incurred. Compensation already paid shall be refunded, irrespective of any claims for damages, if data have been used illegally or if the information has otherwise led to a correction.

5.2 Rectification

5.2.1 Right

Every data subject has the right to apply for the rectification of personal data relating to him if the data are wrong. In addition, the data controller has to rectify incorrect data on his own, as soon as he becomes aware of the incorrectness of the data or the inadmissibility of their processing.

5.2.2 Exceptions

Rectification is not possible if the purpose of a data application does not permit subsequent changes. In such cases, the necessary rectifications shall be effected by means of additional documents.

5.2.3 Deadline

The application for rectification shall be complied with within eight weeks of its receipt and the applicant shall be informed. Otherwise, the data controller has to provide reasons in writing why the requested rectification was not carried out.

5.2.4 Charges

The data subject may not be charged for exercising his right to rectification.

5.3 Erasure

5.3.1 Right

Every data subject has the right to apply for erasure of personal data relating

to him if the personal data are wrong. In addition, the data controller has to erase incorrect data on his own as soon as he/she becomes aware of the incorrectness of the data or the inadmissibility of the processing.

5.3.2 Exceptions

Erasure is not possible if the purpose of a data application does not permit subsequent changes. In such cases, the necessary erasure shall be effected by means of additional documents.

5.3.3 Deadline

The application for erasure shall be complied with within eight weeks after its receipt and the applicant shall be informed. Otherwise, the controller has to provide reasons in writing why the requested erasure was not carried out.

5.3.4 Charges

The data subject may not be charged for exercising his right of erasure.

5.4 Blocking

5.4.1 Right

The ADPA does not foresee any right of data subject to 'block' any use of personal data relating to them.

5.5 Objection

5.5.1 Right

If the use of data is not authorised by law, every data subject shall have the right to raise an objection to the data controller of the data application against the use of personal data because of an infringement of an overriding interest in secrecy deserving protection arising out of his special situation.

The most important requirement for direct marketing is the consent of the customer. In the consent the advertising measures have to be described in detail in accordance with the transparency requirement. According to section 107 Telecommunications Act, direct marketing via short message or email is only allowed if prior consent exists. This is called the 'opt in' principle.

Prior consent is not necessary if the addresser received the contact information in connection with the sale or service to its customers or if the message was carried out only for direct marketing for similar products or if the addressee clearly had the possibility to refuse to object to the use of its contact data ('opting out').

Cold calling is forbidden without prior consent without any exception, both in business-to-business and business-to-consumer communication.

If the inclusion of data in a filing system open to inspection by the public is not mandated by law, the data subject can object at any time and without any need to give reason for his application.

5.5.2 Exceptions

If the data use is authorised by law and the interest in secrecy deserving protection is not violated, the data subject is not able to file an objection.

5.5.3 Deadline
The data controller shall erase the data relating to the data subject within eight weeks from his data application and shall refrain from transmitting the data.

5.5.4 Charges
The data subject may not be charged for exercising his right to object.

5.6 Automated individual decisions
5.6.1 Right
Nobody shall be subjected to a decision that produces legal effects concerning him or which adversely affects him in a significant manner, based on the automatic processing of data intended to evaluate certain personal aspects relating to him.

5.6.2 Exceptions
A person may be subjected to a decision based solely on automatic processing if:
- this is expressly authorised by law;
- the decision is taken in the course of the entering into or performance of a contract, and the request of the data subject for the entering into or the performance of the contract has been satisfied; or
- the legitimate interests of the data subject are safeguarded by appropriate means – such as arrangements allowing him to assert his point of view.

5.6.3 Charges
The data subject may not be charged for exercising his right.

5.7 Other rights
5.7.1 Right
Any data subject has the right to lodge a complaint with the DPA because of an alleged infringement of his rights.

5.7.2 Exceptions
There are no exceptions.

5.7.3 Deadline
There is no deadline.

5.7.4 Charges
The data subject may not be charged.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The data controller is responsible for filing notifications with the DPA.

6.1.2 What

In principle, every automatic data processing activity and every data application has to be notified.

6.1.3 Exceptions

Data applications are not subject to notification if they:

- solely contain published data;
- they consist of managing registers and catalogues that are open to inspection by law for the public, even if a legitimate interest for the inspection must be demonstrated;
- they only contain indirect personal data;
- they are carried out for journalistic purposes; or
- they correspond to a standard application. The Federal Chancellor can issue ordinances designating that particular types of data applications and data transfers constitute standard applications if they are carried out by a large number of data controllers in a similar way and if a risk to the data subject's interest in secrecy deserving protection is unlikely considering the purpose of the data application and the processed categories of data, the categories of data subjects and recipients as well as the maximum period of time for which the data may be stored.

In Austria, 31 standard applications exist. The most important standard applications for companies are the following:

- SA 001: accounting and logistics;
- SA 002: personnel administration;
- SA 022: marketing.

Other standard applications exist, for example, for membership administration or password administration. If a data application falls under the scope of a standard application, it does not need to be notified.

Furthermore, five so called 'model applications' exist: (i) passenger transportation and hotel reservation; (ii) access control systems; (iii) motor vehicle admission; (iv) participation in the joint information system *www.fundamt.gv.at*; (v) participation in the joint information system 'Fund Info'.

In contrast to standard applications, the model applications have to be notified but only their existence, not their content.

Furthermore data applications for the purpose of:

- protecting the constitutional institutions of the Republic of Austria;
- safeguarding the operational readiness of the federal army;
- safeguarding the interests of comprehensive national defence;
- protecting important foreign policy, economic or financial interests of the Republic of Austria or the European Union; or
- preventing and prosecuting crimes,

shall be exempt from the duty to notify, insofar as this is necessary to achieve the purpose of the data application.

6.1.4 When

The notification has to be filed before the start of the data application so it can be registered in the Data Processing Register. The duty to notify also

applies to all circumstances that subsequently lead to the incorrectness or incompleteness of the notification.

6.1.5 How

Notifications have to be filed by completing the relevant paper forms and submitting them to the DPA by post. For this purpose, the data controller has to use an application form which is available under the following address *www.dsk.gv.at/site/6296/default.aspx*. After September 1, 2012, data controllers will have the opportunity to file notifications using an online system.

The notification has to contain the name and address of the data controller; a description of the purpose of the data application; the name of the data application; the data subjects; all data that are processed; the recipients of the data; and the legal grounds for the data processing and transfer. If, for example, the data processing takes place on the basis of consent, this consent has to be submitted along with the notification. A special form regarding the security measures taken has to be attached.

There are four different forms for data applications. The first one – 'information about the data controller' has to contain information about the data controller, its company name, address and the purpose of the data application. The second form is the data application itself, where the data fields have to be included, the legal grounds of the data transfer have to be mentioned and the recipients have to be explained. The third form is the form for the model applications (as explained above). The fourth form is the form which contains the data security measures. This form has to be enclosed with any notified data application.

The DPA shall examine all notifications within two months. If the DPA comes to the conclusion that the notification is insufficient, the data controller shall be ordered within two months after receipt of the notification to correct the insufficiency within a set period.

As already mentioned above, the use of standard applications does not have to be notified with the DPA at all. In contrast, the existence of model applications (not their content) has to be filed with the DPA.

If the order for correction is not complied with on time, the DPA shall, by decision, refuse registration; otherwise, the notification shall be regarded as if it had been filed correctly from the beginning.

6.1.6 Notification fees

No notification fees are charged.

6.2 Authorisation requirements

6.2.1 Who

The data controller has to obtain prior authorisation for the operation of data applications regarding particular types of personal data (see section 6.2.2 below) and certain international data transfers.

6.2.2 What

Data applications are subject to prior approval of the DPA if they include

sensitive data; data related to criminal matters; data revealing information about the credit status of the subject; or if the data application is part of a joint information system. For information about the joint information system please see section 1.4.

Furthermore, authorisation is required for the transfer of personal data to a non-EEA country which does not provide for an adequate level of protection. Please see section 8 below for more details.

6.2.3 Exceptions

Authorisation is not required for the transfer of personal data to an EEA country which provides for an adequate level of protection. Please see section 8 below for more details.

6.2.4 When

See section 6.2.1 above.

6.2.5 How

The application for authorisation has to be submitted as a formal request. There is no standard form to be submitted. The application has to contain all the information required for the DPA to be able to take a decision on the application; in the context of international data transfers outside the EEA, it should contain a description of the transferred data, the recipient and the purpose and legal basis for the transfer. In addition, standard contractual clauses or data transfer agreements shall be enclosed.

If a data application or data transfer is subject to prior authorisation, the data controller has to wait until the DPA has rendered the certificate of registration.

6.2.6 Authorisation fees

A fee of around EUR 20 is charged for authorisation proceedings.

6.3 Other registration requirements

Not applicable.

For information about prior checking please see section 3.5.

6.4 Register

The DPA holds a public data processing register which may be consulted by anyone. This register contains an overview of the basic data of the client (name, address etc) and the reported data applications.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Under the ADPA, it is not mandatory to appoint a data protection officer, which even does not exist in the ADPA at all. As to joint information systems, an entity or person needs to be named to the Data Protection Authority who will be responsible for the system.

7.2 Tasks and powers

Not applicable.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Data transfers from Austria to any other EEA member states are not subject to any additional requirements, as EEA member states are considered to provide an 'adequate level of protection'.

Data transfers to recipients in third countries with an adequate level of data protection do not need to satisfy any additional requirements. The countries which have an adequate level of data protection are enumerated in an ordinance of the Federal Chancellor. Furthermore, any respective decision of the EU Commission is binding on Austria.

8.2 Legal basis for international data transfers

Personal data may be transferred to third countries which do not provide an adequate level of protection without the need to obtain prior authorisation from the DPA if:

- the data have been published legitimately in Austria;
- only data that are indirectly personal to the recipient are transferred or processed;
- the transborder transfer or processing is authorised by regulations that are equivalent to a statute in the Austrian legal system and are immediately applicable;
- only data from a data application for private purposes (eg personal data of relatives, mail correspondence with them from private computers in your household) or for journalistic purposes are transmitted;
- the data subject has, without any doubt, given his/her consent to the transborder transmission or processing;
- a contract between the data controller and the data subject or a third party that has been concluded clearly in the interest of the data subject cannot be fulfilled except by the transborder transmission of the data;
- the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data were collected legitimately;
- the transmission or processing is expressly named in a standard application or model application;
- the data are exchanged with Austrian governmental missions and offices in foreign countries; or
- the transmission or processing are made from a data application that is exempted from notification according to the rules under section 17(3) ADPA. Section 17(3) ADPA stipulates that data applications are not subject to notification if they are necessary for the purpose of protecting the constitutional institutions of the Republic of Austria or safeguarding the operational readiness of the federal army or safeguarding the interests of comprehensive national defence or protecting important foreign policy, economic or financial interests of the Republic of Austria

or the European Union. In all other cases, the data controller has to apply for an authorisation by the DPA.

8.2.1 Data transfer agreements

Data transfer agreements play a big role in transborder data flows. The DPA will grant authorisation for the transfer of personal data to an unsafe country if the data controller gives sufficient guarantees in the form of the conclusion of data transfer agreements that are based on the European Commission's standard contractual clauses. If such agreements based on the submission of the European Commission are used, it is much easier receive authorisation from the DPA.

8.2.2 Binding corporate rules

The use of binding corporate rules (BCRs) is not as common as the use of standard contractual clauses. If a company has established BCRs, they have to be authorised by the DPA for any data transmission. The BCRs have to contain provisions apportioning liability in the case of data breaches and also the purposes of data transmission or data use in general. The Austrian DPA takes part in the mutual recognition process.

8.2.3 Safe Harbour

There is no need for authorisation for the transfer of data to a third country if the US recipient of the data is Safe Harbour certified and the data transfer falls under the scope of the certification. The Safe Harbour certification has to be mentioned in the notification to the DPA.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Data controllers, data processors and their operatives shall keep confidential data that have been entrusted or made accessible to them solely for professional reasons, without prejudice to other professional obligations of confidentiality, unless a legitimate reason exists for the transmission of the entrusted or accessed data.

This confidentiality of data supplements the other statutory obligations of secrecy like banking secrecy or secrecy of the medical profession.

9.2 Security requirements

Measures to ensure data security shall be taken by all organisational units of a data controller or data processor that use data. Depending on the kind of data used as well as the extent and purpose of the use, and considering the state of technical possibilities and economic justifiability, it shall be ensured that the personal data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons.

The DPA does not provide any guidance regarding security requirements. Nevertheless, the notification form regarding security measures (see section 6.1.5 above) can be considered as an indication of which data security measures a data controller is supposed to take.

9.3 Data security breach notification obligation

The introduction of a data security breach notification obligation was one of the most important amendments of the ADPA in 2010.

9.3.1 Who

The data controller has to inform the data subject, but not the DPA.

9.3.2 What

If the data controller recognises or is notified that personal data in his data application have systematically and severely been used unlawfully and the data subject is in danger of damage, proper information to the data subject must be provided. Only if the damage is insignificant may information be omitted.

9.3.3 To whom

The data subject shall be notified.

9.3.4 When

As soon as the data controller becomes aware of the unlawful use.

9.3.5 How

The information shall be provided in an appropriate form. The law does not stipulate a special manner.

9.3.6 Sanctions for non-compliance

The infringement of the information obligation may result in civil liability. In addition to that, there may be an administrative penalty in the amount of up to EUR 25,000.

9.4 Data protection impact assessments and audits

There is no general requirement to carry out data protection impact assessments and audits as such under Austrian law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The DPA may examine data applications in the case of reasonable suspicion of an infringement of the rights and obligations under the DPA. It can ask for access to all documents.

In addition, the DPA may issue recommendations. If a recommendation is not obeyed within the set period, the DPA shall, depending on the kind of violation and *ex officio*:

- initiate an administrative inquiry to check the data application;
- bring a criminal charge;
- in case of severe violations by a private sector data controller, file a lawsuit before the competent court; or
- in the case of a violation by an organ of a territorial corporate body, involve the competent highest authority. This authority shall take

measures within an appropriate period not exceeding 12 weeks, to ensure that the recommendation of the DPA is complied with or inform the DPA of why the recommendation is not complied with.

10.2 Sanctions

Criminal offences

Whoever uses personal data entrusted to or made accessible to him solely due to professional reasons, or that he has acquired illegally for himself, or makes such data available to others, or publishes such data with the intention of making a profit or to harm others, shall be punished by a court with imprisonment up to one year, unless the offence shall be subject to a more severe punishment pursuant to another provision.

Anyone who:

- intentionally and illegally gains access to a data application or maintains an obviously illegal means of access;
- transmits personal data intentionally in violation of the rules on confidentiality and in particular anybody who uses data entrusted to him under the rules regarding data for scientific research and statistics or address data to inform or interview data subjects for other purposes;
- uses or fails to grant information, to rectify or erase personal data in violation of a final judicial decision or ruling;
- intentionally erases personal data incorrectly; or
- gets information by false pretences,

may be punished by a fine of up to EUR 25,500.

10.3 Examples of recent enforcement of data protection rules

The DPA does not see its primary role in enforcing and imposing fines for violations of the data protection rules, but rather tries to make sure that the notification procedure is complied with by data controllers and that, thereby, data controllers evaluate the purposes and scope of their data applications in order to avoid overly intrusive or intensive use of personal data.

10.4 Judicial remedies

A person who was harmed as a consequence of an infringement of some provisions of the ADPA (confidentiality, correction, erasing) may initiate a civil action for damages.

Also the DPA shall, where there is probable cause to believe that a serious data protection infringement has been committed by a private sector data controller, file an action for a declaratory judgment in court.

10.5 Class actions

Class actions under the ADPA are not possible.

10.6 Liability

A data controller or a data processor who has culpably used personal data contrary to the provisions of the ADPA is liable. The data controller or data processor shall also be liable for damage caused by his staff, insofar as their

action was causal to the damage. The data controller shall be exempt from liability if he can prove that the circumstances which caused the damage cannot be attributed to him or his staff. The same applies to the exclusion of the data processor's liability.

An individual can claim damages if a data controller processed data illegally or in violation of the ADPA.

Belgium

Van Bael & Bellis Monika Kuschewsky

1. LEGISLATION

1.1 Name/title of the law

The Law on the Protection of Privacy in Relation to the Processing of Personal Data of 8 December 1992 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*) (the Data Protection Law or DPL), as subsequently modified, and the Royal Decree of 13 February 2001 (*Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Arreté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*) provide the general legal framework for data protection, implementing the Data Protection Directive 95/46/EC (the Directive). The Royal Decree of 13 February 2001 contains more detailed safeguards and procedures for the protection of personal data and also sets out the processing activities that do not need to be notified. Moreover, the right to privacy is enshrined in Article 22 of the Belgian Constitution.

In addition to the Constitution, the DPL and the Royal Decree of 13 February 2001, specific laws also contain provisions on the protection of privacy and personal data, such as:

- the Camera Surveillance Law of 21 March 2007 (*Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's/Loi réglant l'installation et l'utilisation de caméras de surveillance*);
- Collective Bargaining Agreement no 68 concerning the camera surveillance of employees of 16 June 1998 (*Collectieve arbeidsovereenkomst 68 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats/ Convention collective de travail 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail*);
- Collective Bargaining Agreement no 81 concerning the monitoring of electronic communications of employees of 26 April 2002 (*Collectieve arbeidsovereenkomst 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens/Convention collective de travail 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau*);
- the Electronic Communications Law of 13 June 2005 (*Wet betreffende de elektronische communicatie/Loi relative aux communications électroniques*); and

- the Patient Rights Law of 22 August 2002 (*Wet betreffende de rechten van de patient/Loi relative aux droits du patient*).

1.2 Pending legislation

On 26 May 2011 a bill amending the DPL (*Wetsvoorstel tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens wat de administratieve sancties, melding van lekken van gegevens, inzagerecht en informatieveiligheidsconsulenten betreft/ Proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en ce qui concerne les sanctions administratives, la notification de fuites de données, le droit de consultation et les conseillers en sécurité de l'information*) was submitted to the Federal Parliament.

This bill provides for the following changes to the DPL:

- the implementation of the principle of data portability, building on the existing right of access (see section 5.1 below) to allow data subjects to obtain a copy of their personal data in a form that enables them to transfer the data to another service;
- the abolition of the current notification system (see section 6.1 below), which is replaced by an obligation for data controllers to appoint a data protection officer, except for those data controllers that do not significantly process personal data;
- a new power for the Commission for the Protection of Privacy (*Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée*) (the Privacy Commission) to impose administrative fines.
- an obligation on data controllers to notify data breaches to data subjects and to the Privacy Commission, if they affect sensitive data or professional secrecy or data used for authentication.

However, given the limited powers of Belgium's current demissionary federal government, it is unclear when and whether this bill will clear the legislative process.

1.3 Scope of the law

1.3.1 The main players

- The 'data controller' is any natural or legal person, private or public body, which alone or jointly with others determines the purposes and means of the processing of personal data.
- The 'data processor' is any natural or legal person, private or public body, which processes personal data on behalf of the data controller, except for the persons who, under the direct authority of the data controller or the data processor, are authorised to process the data.
- The 'data subject' is an identified or identifiable natural person, meaning that the individual can be directly or indirectly identified, 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.
- The 'third party' is any natural or legal person, private or public body, other than the data subject, the data controller, the data processor and

anyone who, under the direct authority of the data controller or the processor, is authorised to process the data.

1.3.2 Types of data

The DPL only covers personal data relating to natural persons and not data relating to legal persons (eg, companies).

'Personal data' are defined as '*any information relating to an identified or identifiable natural person, ie, the data subject*' and include an individual's name, photograph, telephone number, bank account number, etc.

The DPL distinguishes three categories of special personal data that are subject to stricter processing conditions:

(i) sensitive data, ie, '*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership as well as data concerning sex life*';
(ii) health-related personal data; and
(iii) judicial data, ie, '*personal data relating to litigation that have been submitted to courts and tribunals as well as to administrative judicial bodies, relating to suspicions, prosecutions or convictions in matters of crime, administrative sanctions or security measures*'.

The Privacy Commission determined in its Advice no 17/2008 of 9 April 2008 that biometric data should be considered as personal data. In certain cases biometric data may be considered to be sensitive or health-related data, as they may reveal information regarding the data subject's health or race.

Personal data that have been made anonymous by removing the link to the identifiable person cannot be considered as personal data, provided the anonymisation is absolute and cannot be reversed by any reasonable means likely to be used.

If personal data can be linked to an identified or identifiable person by means of a code, the data will be considered as personal data. Specific provisions on the processing of encoded personal data are contained in the Royal Decree of 13 February 2001.

1.3.3 Types of acts/operations

The DPL covers the 'processing' of personal data, defined as any operation or set of operations which is performed upon personal data, wholly or partly by automatic means, as well as otherwise than by automatic means if the personal data processed are included or are intended to be included in a filing system. The DPL gives the following examples of data processing: the collection; recording; organisation; storage; adaptation or alteration; retrieval; consultation; use; disclosure by means of transmission, dissemination or otherwise making available; alignment or combination; blocking; erasure or destruction of personal data.

A 'filing system' is defined 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. Accordingly, the DPL applies also to non-automatic processing of personal data, provided that such processing is structured. In other words, paper records that are ordered in a structured manner (eg, alphabetically or per keyword) also fall within

the scope of the DPL. However, certain obligations, such as the obligation to notify the processing of personal data to the Privacy Commission (see also section 6.1 below), apply only to the processing of personal data by automatic means.

1.3.4 Exceptions

The processing of personal data by a natural person in the course of a purely personal or household activity falls outside the scope of the DPL.

Moreover, partial exemptions from the application of the DPL exist for certain types of data processing, including processing by public security services, processing for the purpose of implementing anti-money laundering legislation or processing for journalistic, artistic or literary purposes.

1.3.5 Geographical scope of application

The following two categories of data processing operations fall within the geographical scope of application of the DPL:

- The processing of personal data carried out in the context of the effective and actual activities of any data controller permanently established on Belgian territory or in a place where Belgian law applies by virtue of international public law.
- The processing of personal data by a data controller with no permanent establishment in EU territory, if the means used for the processing, which can be automatic or other means, are located on Belgian territory, unless such equipment is used exclusively for the purposes of transit through Belgian territory. Except when the means are used exclusively for the purposes of transit through Belgian territory, the data controller must designate a representative established in Belgium.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Commission for the Protection of Privacy (*Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée*)
Hoogstraat – Rue Haute 139, 1000 Brussels, Belgium
T: +32 (0)2 213 85 40
F: +32 (0)2 213 85 65
E: commission@privacycommission.be
W: *www.privacycommission.be*

2.1 Role and tasks

The Privacy Commission is an independent body and its primary objective is to ensure that every individual's right to privacy is protected when personal data are processed.

The Privacy Commission advises on new laws or other rules relating to the protection of privacy and oversees the processing of personal data by private as well as public entities. In this regard it ensures compliance with the DPL as well as any other applicable laws containing provisions relating to the

protection of privacy in relation to the processing of personal data (see also section 10 below).

In addition to the general division, the Privacy Commission created specialist committees (*Sectoraal Comité/ Comité sectoriel*) that each ensure data protection in a specific sector that is subject to specific rules, eg, a specialist committee was created to oversee the processing of personal data contained in the company register (*Kruispuntbank van ondernemigen/Banque Carrefour des enterprises*). There are currently six specialist committees. In addition to carrying out the normal tasks of the Privacy Commission, the specialist committees can also grant authorisations when this is required by the laws in their specific sector.

2.2 Powers

The Privacy Commission has four main powers:

- to authorise, through its specialist committees, a data processing activity that is subject to special laws;
- to inspect and supervise data controllers on its own initiative or based on complaints;
- to provide information to the public; and
- to issue recommendations.

In particular, the Privacy Commission may carry out on-site investigations and request all necessary information, which the data controller is obliged to provide. The Privacy Commission cannot impose administrative fines, but it may transfer a case to the competent judicial authorities (see also section 10 below).

2.3 Priorities

In 2003, the Privacy Commission adopted its current management plan, setting out the Privacy Commission's priorities. Every year, the Privacy Commission adopts an annual activity report explaining how the Privacy Commission executed the management plan in the preceding year.

In its 2010 activity report, published in September 2011, the Privacy Commission listed the following priorities: eGovernment and the exchange of personal data between different public bodies; the processing of financial data; the technical aspects of data protection; the processing of personal data for purposes of justice and security; and the processing of personal data in the transportation sector.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Consent constitutes one of the possible legal bases for the processing of non-sensitive personal data, sensitive data and health-related data but not judicial data.

The data subject's consent is defined as a *'freely given specific and informed indication of his wishes by which the data subject signifies his or his legal representative's agreement to the processing of personal data relating to the data subject*'.

According to the Privacy Commission, '*freely given, specific and informed*' means that the data subject may not be put under pressure to say 'yes'

to the data processing, that consent must relate to precisely defined data processing and that the data subject must have received all useful information concerning the contemplated data processing.

3.1.2 Form

In principle, the DPL does not require consent to be given in a specific form. However, consent for the processing of sensitive or health-related data must be given in writing.

3.1.3 In an employment relationship

Consent must be given freely. In an employment relationship it may be questioned whether the subordinate position of the employee prevents consent from being truly 'free'.

The Royal Decree of 13 February 2001 prohibits the processing of sensitive and health-related data based on the data subject's written consent if the data controller is the data subject's current or potential employer. For other categories of personal data that may be processed on the basis of the data subject's consent, the Privacy Commission recommends employers not to rely solely on the employee's consent, unless it is clear that the employee is not under any pressure to consent, in particular because the data subject's refusal to consent will not adversely affect his or her position.

3.2 Other legal grounds for data processing

Non-sensitive personal data may be processed if one or more of the following conditions are met:

- 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 before entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the data controller is subject;
- the processing is necessary to protect the data subject's vital interests;
- the processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed; or
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

Processing the three special categories of personal data mentioned in section 1.3.2 above is, in principle, prohibited unless the processing meets certain specific requirements. In particular, sensitive and health-related data may be processed if the data subject has given his written consent, provided that this consent can be withdrawn by the data subject at any time, or if the processing:

- is necessary to comply with labour or social security law obligations;
- is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving

his consent;
- relates to personal data which have been manifestly made public by the data subject;
- is necessary for the establishment, exercise or defence of a right in law;
- is necessary for the purpose of scientific research, provided certain conditions are satisfied;
- is carried out in accordance with the Act of 4 July 1962 on Public Statistics (*Wet betreffende de openbare statistiek/Loi relative à la statistique publique*);
- is necessary for some medical purposes, such as preventative medicine; or
- is necessary with a view to an important public interest.

In addition, health-related data may be processed if the processing is necessary to prevent a specific danger or punish a particular criminal offence, or to promote and protect public health. Moreover, sensitive data may also be processed if the processing is carried out, under certain conditions, by a non-profit-making organisation in the course of its legitimate activities or by an organisation promoting the defence of human rights.

Furthermore, the processing of judicial data is limited to the processing that is carried out:
- under the supervision of a public authority;
- by other persons if the processing of the data is necessary for purposes set out by law;
- by legal or natural persons for the management of their disputes:
- by lawyers exclusively for the defence of their clients' rights; or
- for the purpose of scientific research, provided certain conditions are satisfied.

Consent cannot form the basis for the processing of judicial data.

3.3 Direct marketing and cookies

The processing of personal data for the purpose of direct marketing is subject to the general provisions of the DPL. In addition, the DPL contains specific provisions on direct marketing. In particular, data subjects have the right to object, free of charge and without any justification, to the processing of their personal data for direct marketing purposes (see also section 5.5 below). Moreover, the DPL obliges the data controller to inform the data subject of this right.

In addition, the Law on Electronic Commerce of 11 March 2003 (*Wet betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij/Loi sur certains aspects juridiques des services de la société de l'information*), the Fair Trade Practices Law of 6 April 2010 (*Wet betreffende marktpraktijken en consumentenbescherming/Loi relative aux pratiques du marché et à la protection du consommateur*) and the Royal Decree on Spam of 4 April 2003 (*Koninklijk besluit tot reglementering van het verzenden van reclame per elektronische post/Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique*) contain provisions that protect consumers against unsolicited advertisements.

The use of cookies or equivalent devices is regulated by Article 129 of the Electronic Communications Law of 13 June 2005. Article 129 of the Electronic Communications Law has implemented Article 5(3) of Directive 2002/58/EC on the protection of privacy in the electronic communications sector (the

ePrivacy Directive). Belgium has not yet implemented Directive 2009/136/EC of 25 November 2009, which amends in particular Article 5(3) of the ePrivacy Directive and contains stricter rules on the use of cookies. Although the deadline for the implementation expired on 25 May 2011, Belgium has not yet prepared a draft law for implementation.

Under the present law, in principle, the use of electronic communications networks to store cookies or equivalent devices on a user's or a subscriber's terminal equipment is permitted only if: (i) the user or subscriber has been informed of the purposes of the data processing and of his rights; and (ii) the data controller has offered the user or subscriber the possibility to opt out before installing the cookies.

3.4 Data quality requirements

Data controllers must ensure the fair and lawful processing of personal data. Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

Moreover, only personal data that are accurate, relevant, not excessive in relation to the purposes for which they are collected and/or further processed, kept up to date and kept in a form permitting identification of data subjects for no longer than necessary may be processed.

3.5 Outsourcing

When outsourcing data processing activities to data processors, the data controller is required to select a data processor which will take the necessary security measures, supervise the data processor's compliance with these security measures and enter into a written agreement with the data processor. The written agreement must:

- specify the technical and organisational security measures;
- establish the data processor's responsibility towards the data controller;
- stipulate that the data processor will only act on behalf of the data controller; and
- explain to the data processor that the persons acting under his authority may only process the personal data on the instructions of the data controller, except where an obligation is imposed by, or by virtue of, a law, decree or ordinance.

If the data processor intends to sub-contract the data processing, and this is not explicitly permitted by the contract, the processor should inform the data controller of this intention. In addition, the data processor must ensure that the same obligations that apply to the data processor under the controller-processor agreement also apply to the sub-processor.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use as well as the use of surveillance cameras is subject to the provisions of the DPL.

In addition, the Electronic Communications Law (see section 1.1 above) contains important restrictions on intercepting electronic communications

during transfer, which not only apply to listening in on telephone conversations, but also to monitoring email messages before they reach the recipient. In addition, this Law imposes specific obligations for accessing information stored on a user's computer (or other equipment) using an electronic communications network.

Moreover, the Camera Surveillance Law (see section 1.1 above) contains specific provisions for the installation and use of surveillance cameras. The Camera Surveillance Law distinguishes three types of places where surveillance cameras may be installed, and for each type of place specific rules apply:

- public places, eg, a park or a street;
- private places which may be accessed by the public, eg, a department store or a restaurant; and
- private places which may not be accessed by the public, eg, an apartment building or an office.

Installing surveillance cameras in a public place requires prior authorisation from the local police, whereas mere notification to the Privacy Commission suffices before installing surveillance cameras in private places.

The Camera Surveillance Law also imposes a number of obligations on the installation and use of surveillance cameras, which apply to all three types of places. These include, among others, the obligation to place a standard pictogram to inform individuals of the presence of surveillance cameras and limitations on the viewing of images in real time. The Camera Surveillance Law does not apply to the use of surveillance cameras that is regulated by specific regulation, for instance, the use on the work floor which falls within the scope of Collective Bargaining Agreement no 68 concerning the camera surveillance of employees of 16 June 1998 (see section 3.6.2 below).

3.6.2 Employment relationship

The rules concerning the monitoring of employees are enshrined in two Collective Bargaining Agreements: CBA no 68 and CBA no 81 (see section 1.1 above).

Employers may collect and analyse aggregate data regarding the number and frequency of emails (business or private) transmitted on a company's email system and use of the internet in general, on a regular basis, provided they respect the principles of proportionality, finality and transparency contained in CBA no 81.

However, any monitoring is only allowed for one of the following purposes:

- to prevent unauthorised or defamatory acts, acts that are contrary to morality or that could harm the dignity of another person;
- to protect the economic, commercial and financial interests of the company that are confidential as well as to combat any practices contrary to these interests;
- to ensure the safety and/or the proper technical operation of the IT network systems of the company, including monitoring the costs associated with them and the physical protection of the facilities of the company; or

- to ensure good faith compliance with the principles and rules applicable to the company concerning the use of online technologies.

Moreover, for the last purpose (compliance with principles and rules applicable to the company), CBA no 81 obliges companies to follow specific procedures before identifying the data subject.

With regard to the use of surveillance cameras on the work floor, CBA no 68 provides that employers may use surveillance cameras for the following monitoring purposes:

- to ensure safety and health;
- to protect the company's goods;
- to monitor the production process; or
- to monitor the work of the employees concerned.

If the surveillance cameras are used to monitor the production process with regard to the employees (and not the machines), or to monitor the work of the employees concerned, camera surveillance may, however, not be permanent.

Both CBA no 81 and CBA no 68 lay down procedures on how employees should be informed of the monitoring.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers are responsible for informing the data subjects about the processing of personal data relating to them.

4.2 What

Unless the data subject is already aware of this, the data controller must provide the following information to the data subject:

- the name and address of the data controller and of his representative, if any;
- the purpose(s) of the data processing; and
- the existence of the right to object, free of charge, to any intended processing for the purposes of direct marketing.

Depending on the situation at hand, it may be necessary to provide additional information to guarantee the fair processing of the personal data. Such information may include information on:

- the recipients of the personal data;
- whether a reply to the request for personal data is obligatory or voluntary, as well as the possible consequences of a failure to reply;
- the existence of the right of access to, and the right to rectify, the personal data concerning the data subject; and
- specific information that may be required based on the nature of the processing (for example, for health-related data it may be required that the data subject is informed of the reasons for the processing and the categories of persons that will have access to the data).

If the personal data have been obtained directly from the data subject, the data controller must provide the above information as well as information on the categories of personal data processed.

The data controller is exempt from providing the above information if:

- the data subject is already aware of the information;
- providing this information proves impossible or would require a disproportionate effort; or
- recording or disclosure of the data is expressly laid down by law.

4.3 When

The information should be provided at the time the personal data are recorded. When the data are not obtained directly from the data subject, the information should be provided at the time the personal data are recorded, or when a disclosure to a third party is envisaged, but no later than the first time the data are disclosed.

4.4 How

The DPL does not specify in which form and how the information must be provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Upon request, every data subject has the right to know whether a certain data controller is processing personal data on him and if so, the categories of the personal data, the purposes of the processing and the recipients or categories of recipients to whom the data are disclosed. In addition, the data subject is entitled to receive a copy of the personal data concerned in an intelligible form and all available information as to their source. However, the data controller is not obliged to provide a copy of the full records containing the personal data, rather a list of the personal data themselves suffices.

The data controller who receives an access request from a data subject must inform him of the possibility to enforce his rights before the Privacy Commission or the president of the Belgian court of first instance. The data subject must also be informed of the possibility of accessing the public register which contains notifications of all automatic processing of personal data (see section 6.4 below).

If the personal data are used in an automated decision-making process intended to evaluate certain aspects of his personality, the data subject has the right to be informed about the logical process upon which the automated decision-making is based.

For health-related data, the data controller may choose to give indirect access to the personal data. In that case, a healthcare professional will have access to the data and will report to the data subject.

To exercise the right of access, the data subject must submit a signed and dated request to the data controller, accompanied by proof of the data subject's identity, for example, with a copy of his identity card. The request may be sent by any means of communication.

5.1.2 Exceptions

The right of access may under no circumstances be refused.

5.1.3 Deadline

The data subject can exercise the right to access at any time. In response, the data controller must communicate the information without delay, at the very latest within 45 days after receipt of the request. In case of a second, additional request, the data controller must respond within a 'reasonable delay'.

Access to health-related data that are processed for medical scientific research purposes may be delayed if the communication of the data could harm the research.

5.1.4 Charges

The data subject may not be charged for exercising his right to access.

5.2 Rectification

5.2.1 Right

Any data subject has the right to obtain from the data controller the rectification of incorrect personal data relating to him.

5.2.2 Exceptions

There are no exceptions to the right to rectification.

5.2.3 Deadline

The data controller must rectify the personal data within one month starting from the submission of the data subject's request. Within this one-month period, the data controller must also send notification of the rectifications to the data subject concerned and also to the recipients of the relevant personal data, if these recipients are still known and informing the recipients does not prove to be impossible or require a disproportionate effort.

5.2.4 Charges

The data subject may not be charged for exercising his right to rectification.

5.3 Erasure

5.3.1 Right

Any data subject has the right to obtain the erasure of all personal data relating to him if the data are incomplete or irrelevant with a view to the purpose of the processing, if the recording, disclosure or storage of the data is prohibited, or if the data have been stored for longer than the foreseen retention period.

5.3.2 Exceptions

There are no exceptions to the right to erasure.

5.3.3 Deadline

If the data subject's request is justified, the data controller must erase the personal data within one month. Within this one-month period, the data controller must also confirm the erasure to the data subject concerned and inform the recipients of the relevant personal data, if these recipients are still known and informing the recipients does not prove to be impossible or require a disproportionate effort.

5.3.4 Charges

The data subject may not be charged for exercising his right to erasure.

5.4 Blocking

5.4.1 Right

Any data subject has the right to block any use of personal data relating to him under the same conditions as the right to erasure.

5.4.2 Exceptions

There are no exceptions to the blocking right.

5.4.3 Deadline

Contrary to the right of erasure, the DPL does not provide for a deadline for exercising the blocking right.

5.4.4 Charges

The data subject may not be charged for exercising his blocking right.

5.5 Objection

5.5.1 Right

Any data subject has the general right to object at any time to the processing of personal data relating to him based on substantial and legitimate grounds relating to his particular situation.

In addition, the data subject has the right to object to the processing of personal data relating to him for direct marketing purposes (so-called 'opt-out'). The data subject does not need to motivate or provide any reason for objecting to the use of his personal data for direct marketing purposes.

5.5.2 Exceptions

The data subject does not have the general right to object to the processing of his personal data that are necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or when the processing is necessary for compliance with an obligation to which the data controller is subject or by virtue of an act, decree or ordinance.

No exceptions apply with respect to the right to object to the processing of personal data for direct marketing purposes.

5.5.3 Deadline

If the data subject objects to the (intended) processing of personal data relating to him, the data controller must inform the data subject, within one month, of the action he has undertaken to comply with the data subject's request. If the objection is legitimate, the data controller must stop processing the personal data.

The data controller must stop the processing of personal data for direct marketing purposes upon the data subject's objection.

5.5.4 Charges

The data subject may not be charged for exercising the right to object.

5.6 Automated individual decisions

5.6.1 Right

A decision producing legal effects for a data subject, or materially affecting him, cannot be taken purely on the basis of automatic data processing aimed at evaluating certain aspects of his personality.

In the case of such an automated decision, the data subject has the right to be informed about the logic involved in any automatic processing of data relating to him.

5.6.2 Exceptions

The right does not apply if the decision is taken in the context of an agreement or if it is based on a provision laid down by, or by virtue of, a law, decree or ordinance. However, appropriate measures to safeguard the legitimate interests of the data subject must be included in such an agreement or provision and the data subject must at least be allowed to express his point of view in an effective manner.

5.6.3 Deadline

The data controller must respect the right at all times and must respond to a request for information about the logic involved in the automated processing within 45 days.

5.6.4 Charges

The data subject may not be charged for exercising his right.

5.7 Other rights

5.7.1 Right

Any data subject has the right to request the Privacy Commission to exercise, on his behalf, the right to access, object to, rectify, block and erase with regard to certain types of data processing (see section 1.3.4 above). More specific provisions as to how this right may be exercised are laid down in the Royal Decree of 13 February 2001.

5.7.2 Exceptions

There are no exceptions.

5.7.3 Deadline

There is no deadline.

5.7.4 Charges

The data subject may not be charged for exercising this right.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The responsibility for notification to the Privacy Commission lies with the data controller.

6.1.2 What

In principle, any automatic data processing activity (ie, any processing by automatic means, such as software, computers, etc) must be notified. The Privacy Commission has published guidance on the notification requirements and exemptions on its website.

6.1.3 Exceptions

Automatic processing is exempt from the notification obligation if the sole purpose of the data processing is to keep a public register by virtue of an act, decree or ordinance or if the purpose of the data processing falls within one of the categories listed in the Royal Decree of 13 February 2001 and the conditions applicable to the respective processing category are met. These categories include: payroll management, staff management, the processing of contact details for communication purposes, accounting, the administration of customers and suppliers and the administration of shareholders and partners.

6.1.4 When

Notification must be made prior to starting any automatic processing activity.

If the automatic processing is terminated, the data controller must inform the Privacy Commission. Similarly, if any of the information mentioned in the notification form has changed, the data controller must inform the data subject.

6.1.5 How

Notification may be made online on the Privacy Commission's website, or by completing a hard copy notification form and sending it back to the Privacy Commission. The standard notification forms are available on the Privacy Commission's website.

Within three days of receiving the notification form, the data controller will receive receipt of his notification. Within 21 days the Privacy Commission will send the data controller a personal identification number, a number to identify the notified processing activity and a password to modify the notification. Upon receipt of the notification, the data controller may start the notified processing activity, unless prior authorisation is required (see section 6.2 below).

Notification must be made in either Dutch or French.

Each purpose for which personal data are processed, or each group of connected purposes, requires a separate notification. The notification form includes information, among others, about the name of the processing, the name and address or registered office of the data controller, the purpose(s) of the processing and the categories of the personal data processed.

The Privacy Commission is entitled to demand additional information from the notifying data controller, for instance, regarding the origin of the personal data, the choice of automation technology and the security measures that are put in place.

In 2010, the Privacy Commission received a total of 11,982 notifications, which is an increase of 92 per cent compared to 2009. This number includes

new notifications (11,269), modifications to existing notifications (334) and notifications regarding the termination of a processing activity (376).

6.1.6 Notification fees

It is substantially less expensive to notify online than to notify by hard copy. The fee for an online notification amounts to EUR 25. By contrast, the paper notification costs EUR 125. The fee for modifying an existing notification is EUR 20.

The Privacy Commission only charges one fee for all notifications made by the same data controller and received by the Privacy Commission on the same date. An invoice is sent to the notifying data controller within 21 days after filing the notification form with the Privacy Commission.

6.2 Authorisation requirements

In principle, data controllers do not need to obtain authorisation to carry out a data processing activity. However, authorisation may be required for the transfer of personal data to a non-European Economic Area (EEA) country which does not provide an adequate level of protection (see section 8 below).

In addition, authorisation may be required under specific laws, for instance, for the use of data from the national register (*rijksregister/registre nationale*).

6.3 Other registration requirements

Not applicable.

6.4 Register

The Privacy Commission holds a public register of notified processing operations which may be consulted by anyone, free of charge, at *www.privacycommission.be*. For each processing, the public register contains the same information as is provided in the notification form.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Under the DPL, it is not mandatory to appoint a data protection officer (see, however, section 1.2 above). However, for specific categories of data processing that imply risks to the data subjects' rights and freedoms, the data controller could be required by Royal Decree to designate a data protection officer. However, no such Royal Decree has been adopted so far.

7.2 Tasks and powers

Not applicable.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Data transfers from Belgium to other EEA member states are not subject to any additional requirements because EEA member states are considered to provide an '*adequate level of protection*'.

Data transfers to countries outside the EEA that have not been officially

recognised as providing an adequate level of protection (‘*non-adequate third countries*’) are in principle prohibited, subject to exceptions.

8.2 Legal basis for international data transfers

Personal data may be transferred to non-adequate third countries if one or more of the following criteria is met:

- the data subject has given his unambiguous consent to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken in response to the data subject’s request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the data subject’s interests between the data controller and a third party.
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.
- the transfer is necessary to protect the data subject’s vital interests.
- the transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in that particular case.
- the transfer is authorised by the Belgian Minister of Justice by means of a Royal Decree, on condition that the data controller gives ‘sufficient guarantees’, for example, by concluding a data transfer agreement or adopting binding corporate rules.

8.2.1 Data transfer agreements

The use of data transfer agreements is quite common in Belgium. Authorisation for the transfer of personal data to a non-adequate third country is not required if the data controller gives ‘sufficient guarantees’ in the form of a data transfer agreement that is based on one of the European Commission’s standard contractual clauses for data transfers to third countries. However, the use of such a data transfer agreement must be mentioned in the notification made to the Privacy Commission. Upon receipt of such notification, the Privacy Commission can request receipt of a copy of the data transfer agreement.

In practice, data transfer agreements which are not based on the European Commission’s standard contractual clauses are not in use, because for such agreements an authorisation request must be sent to the Ministry of Justice which will issue an authorisation decision by means of a Royal Decree. There is no standard form to make such an authorisation request, which must be sent to the Ministry of Justice’s Human Rights Service at the following address:

Dienst Rechten van de Mens/Service des Droits de l’homme
FOD Justitie/SPF Justice
Waterloolaan – Boulevard de Waterloo, 115
B-1000 Brussels, Belgium

8.2.2 Binding corporate rules

If a data transfer is based on binding corporate rules (BCRs), such data transfer must be authorised by the Ministry of Justice by means of a Royal Decree. So far, the Ministry of Justice has never adopted such a Royal Decree.

A Protocol, concluded on 13 July 2011 between the Privacy Commission and the Ministry of Justice, (the Protocol) has facilitated the authorisation procedure.

An authorisation request must be sent to the Privacy Commission. The authorisation request may be based on the Article 29 Working Party's Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (WP133).

The Privacy Commission will verify the adequacy of the safeguards for the international data transfer provided in the BCRs, in accordance with the Protocol, and send its advice to the Ministry of Justice. If the advice is favourable, the Ministry of Justice merely verifies that the procedural requirements laid down in the Protocol have been complied with. If so, the Ministry of Justice issues an authorisation decision by means of a Royal Decree. Under the new procedure, authorisation is given by means of an individual Royal Decree, which does not require prior review by the Finance Inspection and the Council of State.

Belgium participates in the so-called mutual recognition procedure. Therefore, if a lead authority in another country has accepted the BCRs, the Privacy Commission will advise the Minister of Justice to authorise the data transfer based on these BCRs.

8.2.3 Safe Harbour

There is no need for authorisation where the personal data are transferred to an organisation that is certified under the US Safe Harbour scheme and the data transfer falls within the scope of that certification. However, the fact that the data transfer is made to a US Safe Harbour certified organisation must be mentioned in the notification form.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The DPL requires data controllers and data processors to ensure the confidentiality and security of personal data. In particular, confidentiality is regarded as an organisational security measure.

9.2 Security requirements

Data controllers and data processors are obliged to ensure that appropriate technical and organisational measures are in place to protect personal data against accidental or unlawful destruction or accidental loss, as well as unauthorised alteration or access and all other unlawful forms of processing.

These measures should ensure an appropriate level of security, taking into account the state of the art in this field and the cost of implementing such measures, and, on the other hand, the nature of the data to be protected and the potential risks.

The Privacy Commission has published a non-legally binding note on

information security on its website as well as a list of standard measures for the security of personal data processing (*Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens/Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*). For instance, the Privacy Commission recommends organisations to allocate responsibility for the security of the data processing, to adopt a security policy and to physically protect the personal data they process, by placing computers and other carriers of personal data in secure premises.

9.3 Data security breach notification obligation

There is no obligation under Belgian law to notify personal data security breaches to the data subjects and/or to the Privacy Commission. Moreover, so far the Privacy Commission has not issued any recommendations in this respect (see, however, section 1.2 above).

9.4 Data protection impact assessments and audits

There is no general requirement to carry out impact assessments and audits as such under Belgian data protection law. However, the Privacy Commission has recommended privacy impact assessments and audits for the deployment of new technologies (see, for instance, the Privacy Commission's recommendation on mobile mapping of 15 December 2010 or the Privacy Commission's recommendation on RFID of 14 October 2009).

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Privacy Commission may adopt opinions and make recommendations, either of its own accord, or at the request of federal or regional governments and legislative bodies, on any matter relating to the application of the fundamental principles of the protection of privacy and personal data, not limited to the provisions of the DPL.

The Privacy Commission may carry out targeted inspections on its own initiative. In addition, the Privacy Commission may investigate complaints received by it. When the Privacy Commission receives a complaint, it will, at the first stage, if it considers the complaint to be admissible, act as a mediator. If mediation between the parties fails, the Privacy Commission can issue an opinion on the merits of the complaint. The opinion may contain recommendations for the data controller.

The Privacy Commission may carry out on-site investigations. In the course of the investigation, the data controller must provide all necessary information upon request and co-operate with the Privacy Commission. The Privacy Commission is also entitled to exercise the right of access and rectification on behalf of a third party (indirect access).

According to the Privacy Commission's 2010 activity report, it initiated 85 audits of individual data controllers in 2010.

10.2 Sanctions

The processing of personal data in breach of the DPL may constitute a criminal offence, penalised with fines of up to EUR 550,000. In addition, a

court may order:
- the confiscation of the media containing the personal data to which the offence relates;
- the erasure of the data; or
- the prohibition to control any processing of personal data, directly or through an agent, for a period of up to two years.

Any repeat offences are punishable by a term of imprisonment from three months to two years, and/or a fine of EUR 550 to EUR 550,000.

Moreover, a person suffering any harm as a consequence of acts infringing the provisions of the DPL can initiate a civil action for damages.

The Privacy Commission does not publish statistics on the number of sanctions imposed. In our experience, data protection infringements currently rarely lead to criminal penalties being imposed.

10.3 Examples of recent enforcement of data protection rules

In 2010, the Privacy Commission received 348 requests for mediation. In 5.9 per cent of the cases that were admissible, the Privacy Commission concluded that data protection rules had been violated. In 98 per cent of these cases, the Privacy Commission obtained a rectification.

In Belgium, individuals are becoming more concerned about the use of their personal data. However, we have not seen many cases where individuals have exercised their rights in courts so far, and when they have, attributed damages were very low. For instance, on 5 March 2009 the Labour Court of Appeal of Brussels ordered an insurance company to pay material damages of EUR 100 and moral damages of EUR 250 after a customer claimed that he had not been granted access to his personal data. The Court also ordered the insurance company to grant access to the insured person to his personal data, under penalty of a fine of EUR 50 for each day of delay.

10.4 Judicial remedies

The Privacy Commission may transfer a case to the Public Prosecutor or bring the case before the Belgian court of first instance. In addition, a person suffering any harm as a consequence of acts infringing the provisions of the DPL can initiate a civil action for damages. In our experience, claims based on privacy and data protection rules are mostly made in judicial proceedings concerning employment disputes.

10.5 Class actions

Class actions are not permitted under Belgian law.

10.6 Liability

The data controller shall be held liable for any damage as a result of an action in violation of the provisions of the DPL. Data subjects that have incurred damage from an action in violation of the DPL may thus claim damages from the data controller. The data controller shall be exempt from liability if he proves that the act which caused the damage cannot be ascribed to him.

Canada

Stikeman Elliott LLP David Elder

1. LEGISLATION

1.1 Name/title of the law

Data protection requirements in Canada may originate from a number of different sources, depending on the nature of the information in question and the jurisdiction from which it was collected, or in which it is held.

Since Canada is a federal state, its legal framework for privacy can be somewhat complex, as statutes exist at both the federal and provincial level, reflecting overlapping constitutional jurisdiction over the subject matter. The privacy law framework is also complicated by the fact that in many Canadian provinces, separate statutes govern each of private sector privacy, public sector privacy and health sector privacy. In addition, unique legislative issues arise with respect to employee privacy.

From a private sector privacy perspective, there are four applicable general privacy/data protection statutes in Canada:

- Personal Information Protection Act, S.B.C. 2003, c. 63 (British Columbia);
- Personal Information Protection Act, S.A. 2003, c. P-6.5. (Alberta);
- An Act respecting the protection of personal information in the private sector, R.S.Q., c. P-39.1. (Québec);
- Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. (Federal).

The federal law, the Personal Information Protection and Electronic Documents Act (PIPEDA), applies to organisations subject to federal regulation, as well as commercial organisations operating wholly in a province that has not enacted its own private sector privacy legislation. However, in employment contexts, PIPEDA applies only to the employees of undertakings that fall under federal legislative competence, leaving a number of the provinces without employee privacy legislation.

With respect to personal health information, there is health information privacy legislation in most of the Canadian provinces; although health privacy is governed in some provinces by its public and private sector privacy statutes rather than a separate sectoral law:

- Health Information Act, R.S.A. 2000, c. H05. (Alberta);
- E-Health (Personal Health Information Access and Protection of Privacy) Act, S.B.C. 2008, c. 38. (British Columbia);
- Personal Health Information Act, C.C.S.M., c. P33.5. (Manitoba);
- Personal Health Information Privacy and Access Act, S.N.B. c. P-7.05. (New Brunswick);
- Personal Health Information Act, S.N.L. 2008, c. P-7.01. (Newfoundland

and Labrador);
- Personal Health Information Act, S.N.S. 2010, c. 41. (Nova Scotia) (passed in late 2010, but not yet in force as of 23 December 2011);
- Personal Health Information Protection Act, 2004, S.O. 2004, c. 3. (Ontario);
- An Act respecting access to documents held by public bodies and the protection of personal information, R.S.Q., c. A-2.1.; An Act respecting the protection of personal information in the private sector, R.S.Q., c. P-39.1. (Québec);
- Health Information Protection Act, S.S. 1999, c. H-0.021. (Saskatchewan).

While Québec lacks health-specific privacy legislation, its public sector privacy legislation also applies to private institutions that receive government funding to operate. Health information held by other commercial enterprises is governed by the province's private sector privacy legislation.

In order to apply in a province, in place of the federal legislation, each piece of provincial privacy legislation is examined against the federal law and the 10 privacy principles it embodies. Only when such legislation is pronounced by the federal Governor in Council to be 'substantially similar' to the federal statute will those laws apply in place of PIPEDA in the province in question. Accordingly, while there are a number of important differences in both content and wording between the various privacy statutes, all cover the same essential principles and obligations.

In addition to these privacy-focused statutes, there are a number of additional laws that impose data protection obligations on certain industrial sectors. For example, telecommunications carriers are subject to restrictions on disclosure of customer information, pursuant to rules created under the Telecommunications Act, S.C. 1993, c. 38. Most provinces have laws respecting consumer credit reporting that place obligations on reporting agencies with respect to the handling of credit information.

1.2 Pending legislation

In September 2011, the Canadian government introduced Bill C-12, the Safeguarding Canadians' Personal Information Act, which was still pending before Parliament at the close of 2011 and contains a number of important changes to PIPEDA, including:
- a new exception that would allow for the use and disclosure, without consent, of personal information in the context of prospective or completed business transactions, such as mergers and acquisitions;
- the exclusion of business contact information from many of the obligations in PIPEDA;
- an apparent enhancement of what will constitute valid consent for the collection, use or disclosure of personal information; appearing to impose on organisations constructive knowledge of the ability of each individual to understand the purposes and consequences of the data collection to which they are consenting;
- a mandatory breach notification framework, requiring the reporting

of material data breaches to the Federal Commissioner (see section 2 below) and the notification of affected individuals and organisations where the breach creates a real risk of significant harm.

Canada's Anti-Spam Legislation (S.C. 2010, c. 23) (CASL) contains a number of amendments to PIPEDA, not all of which are in force at time of writing. Amendments in force as of April 2011 provided the Federal Commissioner with the ability to be more selective about the complaints she decides to investigate, as well as providing the Federal Commissioner with the ability to share information and collaborate in investigations with international and provincial counterparts. Amendments expected to be proclaimed in force sometime in 2012 would permit the Federal Commissioner to take measures against the unauthorised collection of personal information through hacking or the use of computer programs to generate, search for or collect electronic addresses, sometimes known as 'address harvesting'.

1.3 Scope of the law

1.3.1 The main players

With respect to the private sector, the main players vary slightly by jurisdiction.

Federal

The 'organisation' includes an association, a partnership, a person and a trade union, which collects personal information in the course of commercial activities. It does not include (i) any government institution to which PIPEDA applies; (ii) an individual in respect of personal information that the individual collects, uses or discloses only for personal or domestic purposes; (iii) an organisation in respect of personal information that the organisation collects, uses or discloses only for journalistic, artistic or literary purposes.

A 'federal work, undertaking or business' is a work, undertaking or business that is within the legislative authority of Parliament, including those relating to shipping and navigation, railways and canals, air transportation, broadcasting and banking, among others.

Although not a defined term in the legislation, the Schedule to PIPEDA also references personal information transferred to 'third parties for processing.' Such third party processors are not generally seen as being governed directly by the legislation, but rather by contract with the responsible 'organisation', which is legally accountable for compliance with PIPEDA.

There is no defined term equivalent to 'data subject' in European law; however PIPEDA implicitly incorporates as similar concept, as it focuses on 'personal information', which is any information about an identifiable individual, with the exception of certain business contact information.

Provincial private sector

The Alberta and British Columbia (BC) statutes also focus on the 'organisation' responsible for collection, use and disclosure of personal information. These statutes do not define third parties, but again, contemplate the engagement by organisations of other parties or agents, by contract or otherwise.

The Québec law applies to 'persons carrying on an enterprise', which would include legal and corporate persons. The Act speaks explicitly of communicating to third parties information contained in a file opened by such a person.

Provincial health sector

While the precise terminology used varies from province to province, the provincial health sector privacy laws tend to focus on, and apply to, health care 'custodians' or 'trustees', which are generally defined as persons or organisations with custody or control of personal health information in the course of their work. Since the health care field is largely publicly funded in Canada, many health care custodians and trustees are public sector institutions; however, the statutes also capture many private sector health care providers, including, variously, nursing home operators, pharmacies and pharmacists and many physicians and other health care providers paid through provincial health insurance plans. The types of organisations and providers that are governed by health sector privacy legislation, which are often enumerated explicitly in each statute, can vary considerably between the provinces.

Some provinces also recognise in their laws the particular roles played by 'information management service providers,' being organisations that store, process, archive and destroy the records of a custodian or trustee that contain personal health information. At least one of the statutes, the Saskatchewan Health Information Protection Act, also includes the European concept of the 'subject individual.'

1.3.2 Types of data

Federal

'Personal information' means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation.

'Personal health information' refers to information concerning: (i) the physical or mental health of an individual; (ii) any health services provided to an individual or any information collected in the course of providing such health services or incidentally to the provision of such health services; (iii) the donation by an individual of any body part or any bodily substance or derived from the testing or examination of such body part or bodily substance.

Although other sub-categories of personal information are not defined, the Act does recognise that some personal information will be more sensitive than others and imposes stricter obligations with respect to more sensitive data, such as more fulsome disclosures, explicit consent and more robust security safeguards.

Personal information has been found to include biometric information, such as fingerprints and voice prints .

Since personal information must be about an identifiable individual, aggregated and anonymous data is not generally considered to be personal information; however, Canadian courts have held that information will be about an 'identifiable individual' where there is a serious possibility that an individual could be identified through the use of that information, alone or

in combination with other information. For example, IP addresses collected by an Internet Service Provider (ISP) have been found to constitute personal information because the ISP had the ability to link the IP addresses to its customers through their subscriber IDs.

There continues to be an active debate in Canada among interested stakeholders as to whether information that does not identify an individual, but is rather tied only to an internet protocol address or device name should properly be characterised as 'information about an identifiable individual.' The debate is an important one, since the characterisation of any data as personal information is a threshold question for the application of the relevant privacy statutes. The status of data tied to numeric identifiers, which could conceivably be linked to identified persons, has created particularly thorny issues in the realm of online behavioural advertising.

Provincial private sector

While the terminology varies from province to province, the statutes for each of Alberta and British Columbia include definitions of

'personal information' similar to the federal statute. The law for the Province of Québec, defines personal information as any information relating to a 'natural person' that allows that person to be identified.

The Alberta and BC laws also include similar definitions for 'personal employee information' and 'employee personal information' respectively, referring generally to personal information about an identifiable individual that is collected, used or disclosed solely for purposes reasonably required to establish, manage or terminate an employment relationship.

Provincial health sector

While the precise language varies between the various statutes, most provincial laws focus on some definition of 'heath information' or 'personal health information', generally referring to identifying information about an individual that broadly relates to their physical or mental health, the provision of health care to them, etc.

Some of the statutes, such as Alberta's health sector privacy law, also provide for separate definitions and treatment of non-identifying health information and individually-identifying health information, as well as for different sub-types of health information, such as diagnostic, treatment and care information; health services provider information and registration information (basic demographic and content information, as well as health service eligibility).

1.3.3 Types of acts/operations

The federal law applies generally to the collection, use and disclosure of personal information, and the knowledge and consent of the individual is required for each of these, although the consent may be implicit or explicit, depending on the circumstances, including the inherent sensitivity of the information and the reasonable expectations of the individual. Schedule 1 to PIPEDA also recognises that personal information may be transferred to third parties for processing. Although the terms 'transfer' and 'processing' are undefined, the concept is seen

to apply to a very broad range of outsourcing activities, including both automated and manual processing, and whether focused on data processing *per se*, or whether incidentally requiring access to information by the third party. Although information may be transferred to third parties, with the requisite consent of the individual, the organisation transferring the data remains responsible for compliance with privacy and data protection requirements.

The provincial private sector statutes take similar approaches.

Broadly speaking, the provincial health sector privacy laws deal with the collection, use and disclosure of personal health information by a variety of public and private institutions and health care providers within the country's publicly-funded health care system.

1.3.4 Exceptions

PIPEDA applies only to personal information collected, used and disclosed in the course of commercial activity. Data protection obligations do not apply to individuals, in respect of personal information collected, used or disclosed solely for personal or domestic purposes; nor do they apply to organisations in respect of personal information collected, used or disclosed solely for journalistic, artistic or literary purposes. The name, title or business address or telephone number of an employee of an organisation is not considered to be personal information, and is therefore not subject to the requirements of the law. As noted earlier, the federal legislation applies only to employees of federal undertakings, even where that legislation otherwise applies to private sector commercial organisations in a province without its own private sector privacy law.

The private sector laws of Alberta and BC are not restricted to collection, use and disclosure of personal information for commercial activity, applying to any such activity. They include a number of exceptions similar to the federal law, such as personal information used for personal or domestic purposes; artistic, literary or journalistic purposes; and for basic business contacts; however the exemptions in these provincial statutes go much further, also excluding information contained in court files, used by candidates for election or members of the legislature, to name a few.

The Québec law, like the federal law applies only to the collection, use and disclosure of personal information for commercial purposes, and contains exceptions for journalistic, historical or genealogical material collected, held, used or communicated for the legitimate information of the public.

Some of the health care sector privacy statutes contain exceptions, such as excluding stale records (eg the Ontario law does not apply to personal health information after the earlier of 120 years after its creation or 50 years after the death of the subject). A number of these statutes state explicitly that they do not apply to statistical or aggregated health care information.

1.3.5 Geographical scope of application

PIPEDA applies to organisations subject to federal regulation, as well as commercial organisations operating wholly in a province that has not enacted its own private sector privacy legislation. However, in employment contexts, PIPEDA applies only to the employees of undertakings that fall

under federal legislative competence. Separate provincial laws apply to personal information collected, used and disclosed in connection with commercial activity within the provinces of BC, Alberta and Québec. PIPEDA applies to federally regulated undertakings, and in each of the remaining provinces, as well as to personal data that flow across provincial or national borders, in the course of commercial transactions involving organisations subject to PIPEDA or to substantially similar provincial legislation.

PIPEDA has also been found to apply to foreign organisations engaged in commercial activities that have a real and substantial connection between the subject matter, the parties, or the territory to Canada.

Provincial health legislation, or private sector privacy legislation that also extends to private sector heath care providers, exists in all Canadian provinces except Prince Edward Island, and in the Northwest Territories, Nunavut and the Yukon.

1.4 Particularities

The federal law has a somewhat unique structure, in that its privacy elements comprise two parts. One is a schedule containing a flexible, principle-based code created under the auspices of the Canadian Standards Association (CSA); the other is a more traditional statute, but its definitions and provisions are intended to support, and in some cases modify, the CSA standard. As a result, the majority of the obligations that arise under PIPEDA are more in the nature of 'guidelines,' in contrast to the clear obligations that arise under most statutes. That said, they are guidelines that are subject to interpretation by the Federal Commissioner and, upon subsequent application, by the Federal Court of Canada.

The remainder of the Canadian private and health sector privacy statutes follow more traditional, prescriptive statutory formats.

2. DATA PROTECTION AUTHORITY

Federal

Office of the Privacy Commissioner of Canada (the Federal Commissioner)
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3
Toll-free: 1-800-282-1376
T: (613) 947-1698
F: (613) 947-6850
E: Not applicable.
W: *www.priv.gc.ca*

Provincial

The contact details of the nine provincial Privacy Commissioners can be found at *www.priv.gc.ca/resource/prov/index_e.cfm#contenttop*.

2.1 Role and tasks

Federal

The Federal Commissioner is an Officer of Parliament who reports directly to the House of Commons and the Senate. She oversees PIPEDA, which governs the information-handling practices of private-sector organisations everywhere in Canada except BC, Alberta, and Québec. Even in those provinces, PIPEDA continues to apply to the federally regulated private sector, such as telecommunications, banking and transportation, as well interprovincial and international transactions. PIPEDA also applies to the health-care sectors of Nunavut, The Northwest Territories, Prince Edward Island and The Yukon.

Provincial

Each of the provinces of Alberta, BC, Manitoba, New Brunswick, Newfoundland & Labrador, Nova Scotia, Ontario, Québec and Saskatchewan has their own Privacy Commissioner or equivalent to oversee and administer the data protection statutes of that province, consisting variously of public, private and health sector laws of application to activities within the province. Typically, the Commissioners are independent regulators appointed by and reporting to the provincial legislature.

2.2 Powers

Federal

The Federal Commissioner generally functions on an ombudsman model. She has the following core mandate and powers:

- reports to Parliament on issues that touch on the privacy rights of Canadians;
- answers public inquiries and investigates complaints;
- conducts audits of the privacy policies and practices of private sector organisations, and advises them on their obligations;
- conducts and commissions research,
- may take cases to Federal Court, and
- engages in public education and outreach.

The Federal Commissioner has no direct powers to impose fines or make remedial orders, although she can bring applications to the Federal Court to hear a matter considered by her office, and the court can award damages and issue mandatory and injunctive orders.

Provincial

Each of the provincial Privacy Commissioners or equivalents have investigative and educational mandates and powers that are similar to that of the Federal Commissioner; however, unlike the Federal Commissioner, several of the provincial regulators also have the authority to issue mandatory and injunctive orders in order to ensure compliance. The Alberta Commissioner also has the explicit power to require private sector organisations to notify affected individuals of a loss or unauthorised disclosure of their personal information. Other provincial regimes, which

more closely follow the ombudsman model of PIPEDA, do not grant order-making powers to their privacy regulators, instead providing for the issuance of remedial orders by the provincial court or a specialised tribunal, following the completion of an investigation by the applicable Commissioner.

2.3 Priorities

Each year, the Federal Commissioner presents to Parliament a 'report on plans and priorities'. For both 2010-2011 and 2011-2012, the Federal Commissioner identified four priority areas which she feels pose the greatest risks to privacy: information technology, public safety, identity integrity and protection, and genetic information.

The Information and Privacy Commissioner for Ontario has long focused on advocating the concept of 'privacy by design', an approach to protecting privacy by embedding it into the design specifications of technologies, business practices and physical infrastructures.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Consent is not generally included as a formally defined term in Canadian privacy laws; however, the various statutes do contain language that suggests different forms of consent.

PIPEDA generally requires the knowledge and consent of the individual for the collection, use and disclosure of personal information, although there are a number of explicit statutory exceptions. Organisations must make reasonable effort to ensure that the individual is advised of the purposes for which the consent may be used. To be meaningful, the purposes must be stated in a reasonably understandable manner. Consent cannot be required as a condition of the supply of a product or service, unless the consent relates to legitimate purposes that are directly related to the transaction. For example, consent to secondary marketing cannot be made a condition of sale. It is a requirement that consent can be withdrawn at any time.

The Alberta and BC private sector statutes employ a similar approach to consent.

However, the Québec private sector statute explicitly requires that consent to the communication or use of personal information must be 'manifest, free, and enlightened' as well as being given for specific purposes. Consent is valid only for the length of time needed to achieve the purposes for which it was requested.

A number of the health sector statutes also contain provisions setting out the requisite elements of a valid consent, generally requiring that it be knowledgeable and not be obtained through deception. In some cases, the consent must explicitly include an acknowledgement that the individual providing the consent has been made aware of the reasons for disclosure of health information and the attendant risks and benefits. The health sector statutes also tend to include the concept of the reasonable expectations of the individual in question. Given the healthcare setting, many of the statutes include provisions respecting incapacity of individuals to consent, and providing for the consent of substitute decision makers.

3.1.2 Form

The Schedule to PIPEDA contemplates a flexible standard for consent, and allows for both implicit and explicit forms of consent, collected orally, electronically and in writing. The form required can vary according the inherent sensitivity of the information in question, its intended use or disclosure, and the reasonable expectations of the individual in the circumstances. There are a number of statutory exceptions to the requirement for consent.

The provincial private sector standards take a similar approach, also including some statutory 'deemed consents'.

The provincial health sector laws are also generally consistent with their private sector cousins, allowing for explicit and implied consent, but providing that only explicit consent is acceptable in some circumstances, such as where a disclosure of health information is to be made to a person who is not himself a custodian or trustee, or the disclosure is to a custodian or trustee, but is not for the purposes of providing or assisting in the provision of health care.

3.1.3 In an employment relationship

Under PIPEDA, the collection, use and disclosure of employee personal information is subject to the same general rules as with respect to customer personal information; however, the nature of the relationship is fundamentally different, and accordingly the required form of consent, the legitimate purposes and the reasonable expectations of the individual may all be markedly different with respect to employees.

The Federal Commissioner attempts to find a balance between the many legitimate needs of an employer to collect, use and disclose information about employees and potential employees, on the one hand, and the equally legitimate privacy interests of these individuals, on the other. Often, where data handling practices appear to be infringing unduly on the privacy interests of employees, the Federal Commissioner requires that organisations employ the most narrowly targeted, minimally intrusive practices possible in the circumstances. For example, any type of workplace surveillance must be narrowly targeted to demonstrably addressing particular concerns or issues that cannot reasonably be addressed in any other way. The loss of privacy to the individuals must be clearly outweighed by the benefit gained.

Similar approaches are taken in Alberta, BC and Québec.

Moreover, the private sector laws of Alberta and BC explicitly provide for the collection, use and disclosure of personal employee information without consent where:

- such activity is undertaken solely for the purpose of establishing, managing or terminating an employment or post-employment relationship;
- the collection, use or disclosure for the purpose in question is reasonable;
- where the individual is an existing employee, reasonable notice has been provided that such information will be collected, used or disclosed, and for what purposes.

3.2 Other legal grounds for data processing

While Canadian private sector privacy laws do use the term 'processing' with

respect to outsourcing personal information to third parties, the core activities that are regulated by these laws are the collection, use and disclosure of personal information. Generally, consent of the individual is required for each of these activities; however, there are a number of statutory exceptions where information may be collected, used or disclosed without consent. These vary somewhat by jurisdiction, so the federal statute, PIPEDA, will be used as an example.

Under the federal statute, personal information may be collected without consent where:

- the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- it is reasonable to expect that the collection of consent would compromise the availability or accuracy of the information, and the collection is reasonable for purposes related to investigating a breach of an agreement or law;
- the collection is solely for journalistic, artistic or literary purposes;
- the information is publicly available (a term narrowly defined by regulations) and is specified by regulation;
- the collection is made for the purpose of making a disclosure to an investigative body or government institution with lawful authority to request that information, to be used for the purpose of enforcing the law or maintaining national security; and
- the disclosure is required by law.

Personal information may be used without consent:

- for the purposes of investigating a possible contravention of the law;
- for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;
- it is used for statistical or scholarly research or study, where such purposes cannot be otherwise achieved, the information is used in a manner that will ensure its confidentiality, it is impractical to obtain consent and the Federal Commissioner is advised of the use beforehand;
- it is publicly available and specified by regulation; or
- it was collected in the interests of the individual, where it is reasonable to expect that consent to collection would compromise the availability of the information for the purpose of investigating the contravention of a law or agreement, or where the information is required by law

Personal information may be disclosed without consent where it is:

- made to an advocate, notary or a barrister or solicitor who is representing the organisation;
- for the purpose of collecting a debt owed by the individual to the organisation;
- required to comply with a subpoena, warrant or order issued by a court or other person or body with the power to compel the production of information, or to comply with the rules of court respecting the production of records;
- made to a government institution that has requested the information and identified its lawful authority to do so and: (i) indicated that it suspects that the information relates to national security, the defence

of Canada or the conduct of international affairs; (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction; carrying out an investigation relating to the enforcement of any such law, or gather related intelligence

- made to a person who needs the information because of an emergency that threatens the life, health or security of an individual;
- for statistical or scholarly research or study, where such purposes cannot be otherwise achieved, the information is used in a manner that will ensure its confidentiality, it is impractical to obtain consent and the Federal Commissioner is advised of the use beforehand;
- made to an institution whose functions include the conservation of records of historical or archival importance, and the disclosure is made for the purpose of such conservation;
- made after the earlier of 100 years after the record was created or 20 years after the death of the individual to whom the information relates;
- of information that is publicly available and specified in the regulations;
- made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or contravention of the law, or is otherwise required by law.

As noted above, additional exceptions to the consent requirement apply in some jurisdictions with respect to the collection, use and disclosure of employee personal information.

The various health sector privacy statutes also provide statutory authority to collect, use and disclose personal health information, without consent, in a wide range of circumstances.

3.3 Direct marketing and cookies

Under the private sector privacy laws, the collection, use and disclosure of personal information for direct marketing purposes is governed by the general scheme of these Acts, therefore requiring the consent of the user. As noted above, organisations cannot require direct marketing consent as a condition of the supply of a product or service. In practice, from a privacy law perspective, the type of consent used with respect to direct marketing has tended to be an opt-out consent; however, special federal rules and laws apply with respect to telephone solicitation and commercial electronic messages.

The Québec private sector law is unique in Canada in that it explicitly allows businesses to use and disclose 'nominative lists' (list of names, addresses or telephone numbers of natural persons) without the consent of the individuals concerned, provided that the lists are used solely for 'commercial or philanthropic prospection', ie direct marketing, and provided that the individual concerned may opt-out of the list.

The Canadian Radio-television and Telecommunications Commission, an independent federal regulatory agency that oversees broadcasting and telecommunications in Canada, has created unsolicited telecommunications rules respecting unsolicited voice, fax and automatic dialling-announcing device (ADAD) communications. Only the use of ADADs for commercial solicitation is prohibited; other methods of telemarketing are regulated, and

subject to restrictions relating to such matters as permitted calling hours, caller identification and contact requirements and the maintenance of telemarketer-specific do-not-call lists.

Telemarketers are also subject to a national Do Not Call List, and are prohibited from making calls to consumers included on the list. Exemptions exist for calls made to a consumer with which the telemarketer has an existing business relationship, as well as to calls made by registered charities, newspapers, political parties and market research and survey organisations. The rules do not apply to business-to-business calling.

With respect to other types of electronic messages, Canada has recently enacted anti-spam legislation, which is expected to come into force sometime in 2012. Canada's Anti-Spam Legislation (S.C. 2010, c. 23) (CASL) generally prohibits the sending of commercial electronic messages (broadly defined to include SMS, email and social networking messages) without the explicit consent of the recipient. A number of exemptions exist, including, for example, exemptions for existing business relationships, conspicuous publication of an electronic address and responses to requests for estimates or quotations. The Act also amends PIPEDA to prohibit crawling the internet to collect addresses to build email lists ('address harvesting').

With respect to cookies, there is no explicit mention of these tools in any of the private sector statutes, all of which apply only to the collection, use and disclosure of 'personal information.' The Federal Commissioner has determined that first party cookies are 'personal information' within the meaning of PIPEDA where the information contained therein could be readily linked to an identifiable individual. Most recently, guidelines released by the Federal Commissioner indicate that she takes the position that the information involved in online tracking and targeting for the purpose of serving behaviourally targeted advertising to individuals will generally constitute personal information, based on the assumption that there will often be a serious possibility that such tracking information could be linked to an individual.

Where behavioural data, such as cookies, are considered to be 'personal information' advertisers can only collect, use or disclose such information in accordance with privacy laws. This means that online advertisers can only track personal information if the individual is made aware of the tracking and its purposes, and provides his or her consent.

Consent to online tracking, such as through cookies, tends to be obtained in Canada through the privacy policies of internet service providers, website owners and advertisers, all of which tend to rely on implied consent models. The Federal Commissioner has accepted an opt-out approach provided that cookies do not contain sensitive information like medical data, and provided that the organisation setting the cookie is transparent about its practices and provides for an easily executed, persistent and permanent op-out. For standard first and third party cookies the availability of browser tools to accept or deny cookies has not to date been a particularly relevant factor in Canada to determine whether the individual has provided the necessary consent for the use of cookies and the collection of the information that they comprise; however, the Federal Commissioner has indicated that

organisations should not employ tracking technology, such as 'zombie cookies' or supercookies, if no opt-out mechanism exists.

3.4 Data quality requirements

Canadian privacy laws, governing both the private and health sectors, are generally consistent with EU requirements respecting data quality, incorporating requirements that limit the collection, use and disclosure of personal information to that which is necessary for the legitimate purposes identified by the responsible organisation. Such information is to be used and disclosed solely for these purposes and must be anonymised or destroyed when no longer required to fulfil those purposes. Personal information must be as accurate, complete and up-to-date as necessary to fulfil the identified purposes.

3.5 Outsourcing

Canadian privacy laws generally permit the transfer of personal information to third party service providers, subject to certain restrictions and protections. As noted, under the various federal and provincial privacy laws, organisations, enterprises and health care custodians or trustees are each ultimately responsible for personal information within their care or control, including information that is transferred to a third party for processing. Organisations must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Such protections include the requirement to protect personal information by security safeguards appropriate to the sensitivity of the information, including physical, organisational and technical measures. Outsourcing agreements therefore typically require adherence to these safeguards, and often include audit rights, indemnities and rights to liquidated damages in the case of non-compliance with the requirements of privacy legislation.

Special restrictions and obligations arise under several of the statutes with respect to outsourcing that involves access to, or storage of personal information outside of Canada, and in some cases, outside of a province (see section 8 below).

Ontario's health sector law, PHIPA, requires express consent for any disclosure or transfer to a non-custodian, which would include service providers. The associated regulations impose additional requirements and restrictions on service providers. They are prohibited from disclosing any information and their use is restricted to purposes necessary for the provision of the service. Furthermore they must ensure that their employees agree to these conditions.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use, as well as the use of surveillance cameras is considered to be a collection of personal information and is governed by the general requirements of the private sector privacy laws, including the need for the consent of the affected individual, unless inappropriate in the circumstances. Section 184 of the Criminal Code generally prohibits the interception of private communications, which could conceivably include

email; however, the prohibition does not apply where one of the parties to the communication has consented (as many employees do when accepting terms of employment, or internet users do in accepting terms of use from their ISP). Still, the Criminal Code serves as a strong safeguard to private electronic surveillance in other circumstances. Beyond this criminal provision and the general privacy laws, there are no specific laws or statutory provisions dealing explicitly with electronic monitoring, and there are no definitive Canadian court rulings that clearly define the limits of acceptable electronic monitoring, although there are many decisions respecting the ability of the state to conduct such monitoring, based on Canada's constitutional guarantee to be free from unreasonable search and seizure.

Video surveillance is generally considered to be a highly privacy-invasive technology, and therefore each of the private sector Privacy Commissioners requires a clear and legitimate business need for the surveillance, that cannot be adequately addressed through other less invasive measures. The Federal Commissioner and provincial Privacy Commissioners for Alberta and BC have jointly issued guidelines on the use of overt video surveillance, and several have issued their own guidelines on covert surveillance, where the restrictions on use are particularly stringent, including:

- Information to be used only for narrowly tailored and specified business purpose and for no other purpose (eg if required for security purposes, cannot be used for employee performance monitoring).
- The use and viewing range of the camera should be as limited as possible, precisely targeted on areas of concern, and should not be focused on areas with a high expectation of privacy (eg washrooms).
- Any recorded images should be stored securely and destroyed when no longer required for business purposes.
- Cameras that are turned on for limited periods are preferable to 'always on' surveillance.
- Sound should not be recorded unless there is a clear need to do so.

Under PIPEDA, the Alberta and BC statutes, video surveillance need not be recorded in order to be subject to the laws of these jurisdictions; however, the Québec statute seems to apply only to recorded information.

3.6.2 Employment relationship

Due to the nature of the employment contract, it can be easier to satisfy legal needs for consent to monitoring where employees are concerned. On the other hand, there are some businesses which take the position that all behaviour on 'company time' or on workplace equipment and systems is proprietary to the business, resulting in much greater surveillance of employees than of non-employees.

In addition to the general issues raised above, there is some uncertainty as to applicability of the Criminal Code to the monitoring of employee email, since the provision prohibits only the interception of 'private communications', and it is unclear whether an email communication made on an employer's computer and system should properly be considered to be 'private.' It is also worth noting that, in addition to the general legal framework discussed above, restrictions on employee monitoring may also be imposed through collective agreements.

Notwithstanding what some see as a lack of clarity as to the legal obligations

and requirements respecting electronic monitoring, the monitoring of email and internet use by employees is quite common in Canada, with companies generally obtaining such consent through a combination of employee email and privacy policies, terms of employment and online notices. Whether a given type of employee monitoring will comply with the applicable legislative privacy standard will depend on a wide range of factors, including the nature and purpose of the monitoring, the uses made of the resulting information, the type and frequency of notice to the employees and the form and adequacy of the consent; however, the law generally seems to consider that an employee whose employer has posted a policy or uses an employment contract that indicates that employee use will be monitored, will have very limited expectations of privacy with respect to their use of employer computers, systems and email accounts. With respect to email, there is some indication in jurisprudence that a greater expectation of privacy may be afforded to employees using internet mail, as opposed to an internet account hosted by the employer, even where the internet account may be accessed from a work computer.

4. INFORMATION OBLIGATIONS

4.1 Who

A core requirement of each of the private sector privacy laws is that the responsible organisation or enterprise must identify to affected individuals the purposes for which their personal information will be collected, used and disclosed.

4.2 What

The health sector privacy laws generally take the same approach, although many allow for the collection, use and disclosure of a fair amount of personal health information for explicitly-defined health-related purposes, without the need for notices, or even consent. Given that the concepts of knowledge and consent are inherently linked, even without a statutory requirement to provide certain information to an individual (as is the case with Ontario's PHIPA) the requirement for consent implicitly includes a requirement to notify the affected individual of the intended purposes.

The private sector laws also require that organisations must be open about their policies and practices with respect to the management of personal information, making such documents readily available to individuals.

In situations involving the transfer of personal information outside the country, such as in an outsourcing arrangement, the Alberta statute requires that the organisation's policies and practices must specify the countries outside Canada where such outsourcing is likely to occur, as well as the purposes for which the foreign service provider has been authorised to process data on the organisation's behalf. In the case of offshore outsourcing, the Federal Commissioner has required organisations to notify affected individuals of this outsourcing, as well as the fact that such outsourcing will make the data stored and processed offshore subject to the legal jurisdiction of the host country, where it may be accessed by domestic law enforcement and security personnel.

In addition to the purpose information discussed above, under the private sector laws, organisations must make readily available information about their personal

information management policies and practices. This information must include:

- the name, title and address of the person accountable for the organisation's compliance with privacy rules;
- information about how to gain access to personal information held by the organisation;
- a description of the type of personal information held by the organisation, along with a general account of its use; and
- identification of any personal information made available to affiliated organisations, such as subsidiary corporations.

4.3 Exceptions

There are a number of exceptions under each of the private sector statutes where the knowledge and consent of the individual are not required for each of the collection, use or disclosure of personal information (see section 3.2 above). Accordingly, the requirement to identify the purposes for such collection, use or disclosure does not apply in such circumstances - although as a practical matter, most privacy policies explicitly account for these exceptions, essentially obtaining consent in advance for these uses, without the need for further consent.

Each of the Alberta and BC private sector statutes also empowers the relevant Information and Privacy Commissioner to authorise an organisation to disregard one or more requests by an individual for access to records and provision of information, where the requests are deemed to be frivolous of vexatious, or where, because of their repetitions or systematic nature, the request would unreasonably interfere with the operation of the organisation.

4.4 When

Generally, information describing the purposes for the collection, use or disclosure should be provided before the individual consents or the information is collected, used or disclosed.

There is no fixed timeline for providing information about an organisation's policies and practices relating to the management of personal information, although the law requires that individuals should be able to acquire the information without unreasonable effort, suggesting that the information should be made available as soon as possible after the request.

4.5 How

There are no fixed formats for the provision of the information noted above.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Under Canadian privacy law, individuals generally have the right to be informed of the existence, use and disclosure of their personal information, and shall be given access to that information on request. Organisations are also required to assist individuals, as requested, in preparing a request to the organisation.

5.1.2 Exceptions

By law, requests for access to personal information held by organisations must be in writing, so requests made other than in writing need not be honoured.

An organisation is not required to give an individual access to personal information if doing so would likely reveal personal information about a third party; however, if the third party information is severable from the record, organisations are required to sever the third party information before giving the individual access.

Organisations are also not required to provide access to personal information if:

- the information is protected by solicitor-client privilege;
- to do so would reveal confidential commercial information;
- to do so could reasonably be expected to threaten the life or security of another individual;
- the information was collected without consent, in circumstances where obtaining consent would have compromised the availability or accuracy of the information;
- the information was generated in the course of a formal dispute resolution process.

Again, the expectation is that with respect to confidential commercial information or a potential threat to the life or security of another, if the information may be severed, it will be before providing access to the individual.

Where an individual requests that the organisation inform it about any disclosure of information to a government institution as part of an investigation of a contravention of a law or a national security matter, or the existence of any information concerning a disclosure related to a subpoena, warrant or other court order, or the individual requests access to records that would reveal this information, the organisation is required to notify the relevant government institution in writing and without delay, and shall not respond to the individual for at least 30 days. The institution in question may object to the release of the data in question, and the organisation may be prohibited from providing the information.

5.1.3 Deadline

Access requests may be made at any time, but organisations are required to respond with due diligence, and in any case not later than 30 – 45 days after receipt of the request, depending on the jurisdiction. An organisation may extend the time limit for a maximum of another 30 days if meeting the time limit would unreasonably interfere with the activities of the organisation or the time required to undertake any consultations would make the time limit impractical to meet. The time may also be extended for as long as is necessary to convert the personal information to an alternative format, for individuals with sensory disabilities. Failure to meet the response deadline results in a deemed refusal of the organisation to the access request.

5.1.4 Charges

Generally access is to be provided at minimal or no cost to the individual. Organisations may respond to an access request at a cost to the individual

only if the organisation has advised the individual of the approximate cost and the individual has advised the organisation that he nevertheless wishes to pursue the request.

Under the Alberta and BC statutes, organisations may not charge a fee in respect of a request for personal employee information. The Québec private sector legislation prohibits charging a fee for access, but allows for a reasonable charge requesting the transcription, reproduction or transmission of the information in question.

5.2 Rectification

5.2.1 Right

Individuals are able to challenge the accuracy and completeness of personal information that an organisation holds about them, and have it amended, as appropriate.

5.2.2 Exceptions

Under the Alberta and BC laws, an organisation is prohibited from correcting or otherwise altering an opinion, including a professional or expert opinion. Organisations are only required to correct records if they are satisfied on reasonable grounds that an individual's request for rectification is valid. Where no correction is made, the organisation must annotate the file with the correction that was requested but not made.

Under Ontario's health privacy law, a custodian is not required to correct a record of personal health information if it consists of a record that was not originally created by the custodian, and the custodian does not have sufficient knowledge, expertise and authority to correct the record. A custodian is similarly not required to correct a record if it consists of a professional opinion or observation that a custodian has made in good faith about the individual. Newfoundland and Labrador's health privacy law includes similar exceptions, but also provides that a record need not be corrected if the custodian believes in good faith that the request is frivolous, vexatious or made in bad faith. Pursuant to Manitoba's Personal Health Information Act, trustees appear to have an open discretion to refuse to correct a record, and are merely required to notify the individual of their reasons and add a 'statement of disagreement' to the individual's file.

5.2.3 Deadline

Information is to be corrected as soon as is reasonably possible, but no hard deadline is set out in the statutes.

5.2.4 Charges

Under the Alberta and BC statutes, organisations may not charge a fee in respect of a request to correct an error or omission in their personal information.

5.3 Erasure

There are no particular requirements to erase (as opposed to correct) data; however, the laws require that information be retained for only so long as is

necessary to fulfil the purposes for which it was collected, after which it is to be destroyed, erased or made anonymous.

5.4 Blocking

There are similarly no particular requirements to block the use of personal information, but all such use is subject to the consent of an individual, which may be withdrawn at any time, subject to legal or contractual restrictions and reasonable notice.

5.5 Objection

There are no particular rights to object to the processing of personal data; however as noted above, consent may be withdrawn at any time.

The law also requires that individuals be allowed to address a challenge concerning an organisation's compliance with the law in question.

5.6 Automated individual decisions

There are no statutory restrictions with respect to automated individual decisions.

5.7 Other rights

There are no other pertinent rights relevant to individual access.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

There are no registration requirements under Canadian privacy laws that are comparable to European law.

6.2 Authorisation requirements

There are no authorisation requirements under Canadian privacy laws that are comparable to European law.

6.3 Other registration requirements

Not applicable.

6.4 Register

Not applicable.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Organisations are required to designate an individual or individuals who are accountable for their compliance with privacy law requirements. Typically, this responsibility is assigned to the organisation's Chief Privacy Officer, but it need not be.

7.2 Tasks and powers

Canadian privacy laws give no particular powers to privacy or data protection officers.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The federal and BC private sector privacy laws are silent on the subject of international data transfers; however, like all transfers for processing, the disclosing organisation remains responsible for the protection of any data so transferred, and is required to use contractual and other means to provide a comparable level of protection while their information is being processed by a third party. Several of the Privacy Commissioners have issued guidelines suggesting the types of contractual and other arrangements that would be expected of organisations entering into international outsourcing arrangements.

One aspect of security that cannot be governed by contract occurs when information is outsourced to another country, at which point it becomes subject to the legal jurisdiction of that country, including any applicable laws respecting access to records and data by that foreign government. Each of the Privacy Commissioners in Canada with private sector responsibility requires that organisations outsourcing to foreign countries obtain the consent of the affected customers (often, via implied consent to a privacy policy or general terms of use), including an explicit disclosure that information sent cross-border or offshore will be subject to the legal jurisdiction of those countries, and may be accessed under those foreign laws.

In Alberta, although the transfer of information outside of the country is not specifically prohibited, organisations that use service providers outside of Canada have additional requirements placed on them. In such cases, organisations must develop specific policies and practices which include: information regarding the countries, other than Canada, in which personal information is collected, used, disclosed or stored; and the purposes for which the service provider has been authorised to collect, use or disclose personal information. In the Québec private sector legislation, there are similarly no specific prohibitions on the transfer of personal information outside the province, but any person who communicates or entrusts personal information outside of Quebec must take reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those where disclosure is permitted without consent in the Act. Similarly, in the case of nominative lists the persons concerned must have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list. If the organisation cannot ensure that it meets these conditions then the enterprise must refuse to disclose the information to the organisation outside Quebec.

Although it is primarily directed at the public sector, Nova Scotia's Personal Information International Disclosure Protection Act also applies to private sector service providers retained to perform services for a public body. The law generally requires that public bodies (and their service providers) ensure that personal information in the control or custody of public bodies be stored and access only in Canada. There are limited exceptions to this requirement, including where the consent of the individual is obtained, or where the head of a public body considers that storage or access outside the country is required to

meet the necessary operational requirements of that body.

Similar to the approach in the private sector privacy laws, the health sector privacy legislation in most of the provinces permits transfers of personal health information outside Canada, but generally imposes limits on the purposes for which such transfers may be made, as well as requirements to ensure that the Canadian custodian maintains control over the information at all times and that the transferred data are protected by appropriate policies, procedures and security safeguards. All permit such transfers with the consent of the affected individuals.

BC's E-Health (Personal Health Information Access and Protection of Privacy) Act is somewhat different from the laws in the other provinces in that it allows for the imposition of restrictions on the transfer outside Canada of personal health information that are specific to particular databases. The responsible Minister is empowered to designate a database of personal health information as a 'health information bank' and may identify in that designation the purposes for which personal health information contained therein may be disclosed outside the country, drawing from a list of acceptable purposes relating to the provision of health care services.

8.2 Legal basis for international data transfers

See section 8.1 above.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Personal information is subject to an implicit requirement of confidentiality, in that it may only be disclosed to third parties with the consent of the individual concerned.

9.2 Security requirements

Canadian privacy laws generally require that personal information held by an organisation be protected by security safeguards appropriate to the sensitivity of the information. Safeguards are to protect against loss or theft, as well as unauthorised access, disclosure, copying, use or modification. Methods of protection should include physical, organisational and technological measures. That said, the laws stop short of imposing detailed security requirements.

The Privacy Commissioners have variously issued guidelines and self-assessment tools relating to best practices for security. Moreover, a body of case law is developing from Privacy Commissioner decisions respecting complaints, which further suggest what the current standards for data security may be. For example, many of the Commissioners have suggested that encryption is the minimum standard required where personal information is stored on a laptop or other portable digital device. In assessing the adequacy of security measures in any particular case, privacy regulators also have regard to the existence of external standards, such as those applicable to the payment card industry, as a means of benchmarking compliance.

9.3 Data security breach notification obligation

While all of the Privacy Commissioners strongly encourage organisations

to voluntarily notify the Commissioners in the event of a data breach (and many of them have forms and processes for such reporting), only five statutes actually mandate such reporting: Alberta's private sector privacy law, and the health sector privacy laws of Ontario, New Brunswick and Newfoundland and Labrador. At the time of writing, a bill that would add a breach notification provision to the federal private sector privacy law was before Parliament.

In her most recent (June 2011) report to Parliament, the Federal Commissioner noted that the number of voluntary breach notifications received in 2010 had dropped from the previous year, which in turn had shown a decrease from 2008. Only 44 notifications were received in 2010, and about two-thirds of these came from financial institutions. The Alberta Information and Privacy Commissioner similarly noted that the number of self reported breaches for 2009-2010 had decreased by 50 per cent from the previous year. Only 15 reports were received. In her most recent annual report, the Ontario Information and Privacy Commissioner had received 95 self-reported breach notifications in 2010, down slightly from 101 the previous year.

Alberta's PIPA is currently the only breach notification requirement that applies to private sector organisations, and at the time of writing, the breach notification amendment had been in place for less than 18 months.

9.3.1 Who

Organisations in control of personal information are required to provide notification of a material breach, whether or not they have physical possession; accordingly, if an outsourcer used by an organisation suffers a data breach, it is the disclosing organisation, not the outsourcer that must notify.

9.3.2 What

By way of example, under the Alberta statute, organisations must provide the Information and Privacy Commissioner with the following details when reporting a breach:

- a description of the circumstances;
- the relevant date or time period;
- a description of the personal information involved;
- an assessment of the risk of harm to individuals resulting from the breach;
- an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the breach;
- a description of any steps that the organisation has taken to reduce the risk of harm to individuals;
- a description of any steps taken to notify individuals of the breach; and
- the name and contact information for a person who can answer the Commissioner's questions about the breach.

Regulations enacted under the New Brunswick law requires the provision of similar information to affected individuals (omitting the number of individuals potentially affected or the assessed risk of harm), as well as the date on which the breach came to the attention of the custodian. While the Ontario and Newfoundland and Labrador statutes or regulations do not provide for such details, the Ontario Commissioner has published guidelines

suggesting that similar information be provided upon breach notification.

9.3.3 To whom

Notification requirements vary by province, with some jurisdictions requiring notification only to the relevant Privacy Commissioner, who may then require notification of individuals (Alberta) some requiring notification to affected individuals (Ontario) and still others requiring notification to both (New Brunswick, Newfoundland and Labrador).

9.3.4 When

Alberta's PIPA requires an organisation to notify the Information and Privacy Commissioner of Alberta without unreasonable delay of any incident involving the loss of or unauthorised access to or disclosure of personal information within the organisation's control, where 'a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorised access or disclosure.'

The Act in turn empowers Alberta's Commissioner to require an organisation to notify individuals to whom there is a real risk of significant harm stemming from a breach, within a time period and subject to any conditions that the Commissioner may determine. The Commissioner may also require an organisation to provide any additional information required to determine when individuals should be notified, or to determine compliance with any conditions.

Ontario's Personal Health Information Protection Act requires that health information custodians notify affected individuals at the first reasonable opportunity if their personal information is stolen, lost, or accessed by unauthorised persons, apparently without regard to the seriousness of the breach.

By contrast, New Brunswick's Personal Health Information Privacy and Access Act and Newfoundland and Labrador's Personal Health Information Act relieves custodians of the requirement to notify where they reasonably believe that a breach will not have an adverse impact on the well-being of the individuals concerned, or the provision of health care or other benefits to those individuals, or would lead to the identification of the individual to whom the information relates. However, even in such cases, the Newfoundland statute contemplates that in such cases, the Commissioner might nevertheless recommend notification of the affected individuals.

9.3.5 How

In cases where individuals must be advised, the statutes are silent as to what method needs to be used to alert the affected parties, but in many cases, organisations use a combination of letter mail and live operator outcalls (the latter tend to be used in particular where the organisation wants to respond to concerns immediately). Regulations enacted in New Brunswick explicitly allow for providing notice in person, by telephone or in writing.

In Alberta, both notifications to the Commissioner and to affected individuals are to be made in the form prescribed by the regulations. Many of the Privacy Commissioners make available forms for this purpose, as well as guidebooks with key numbers to call and information about best practices.

9.3.6 Sanctions for non-compliance

Under the Alberta statute, failure to notify the Commissioner in the event of a breach or to adhere to a related order of the Commissioner to notify individuals constitutes an offence and is punishable by fines of up to $100,000 for corporations. The New Brunswick, Newfoundland and Labrador and Ontario statutes do not contain any offences or fines directly applicable to a failure to report a data breach, but contain general fines applicable to failing to protect personal information with adequate security safeguards.

9.4 Data protection impact assessments and audits

There are no provisions in the privacy sector privacy laws requiring that organisations carry out privacy impact assessments or audits, although they may be ordered to do so by the relevant Privacy Commissioner. The Federal Commissioner also has the power to audit the personal information protection practices of an organisation, if there are reasonable grounds to believe that the organisation is non-compliant. The Alberta and BC Commissioners have broad investigation and inquiry powers.

However, all of the private sector Privacy Commissioners strongly encourage organisations to perform privacy impact assessments when introducing new products and services, and make impact assessment tools available on their websites.

In addition, requiring organisations to undergo and file, at their own expense, periodic third party compliance audits is becoming a common feature of high-profile complaint settlements.

In the health care world, a number of the provincial statutes, including those for Alberta and New Brunswick, require custodians/trustees to prepare a privacy impact assessment with respect to proposed administrative practices, information systems or data matching to examine how such an initiative may impact individual privacy. Typically, these must be submitted to the relevant Commissioner for review and comment before implementing any such new measure.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

A wide range of enforcement tools are contained in the various Canadian privacy statutes, with the nature of these tools varying considerably between various jurisdictions. Some statutes, like Alberta's private sector law, provide the Privacy Commissioner with broad investigative and order-making powers, include a number of offences punishable by material fines and provide a statutory right of damages. Others, like the Federal privacy law, create more of an ombudsman model, where the Commissioner has only the power to investigate and make recommendations, but cannot make orders.

Ultimately, a great deal of enforcement rests on the desire of companies to avoid the adverse publicity that tends to flow from privacy non-compliance; particularly from breaches.

10.2 Sanctions

Canadian privacy statutes tend to rely on quasi-criminal offences, which are

prosecuted by the Attorney General on behalf of the state before a court of competent jurisdiction. There are no direct powers afforded to the Privacy Commissioners to levy fines or administrative penalties.

10.3 Examples of recent enforcement of data protection rules

Most privacy complaints and investigations in Canada tend to be settled and resolved, although some certainly proceed to litigation. Typically the settlements contain a number of undertakings to change practices going forward, and increasingly include undertakings to have periodic compliance audits performed, at the organisation's expense, for filing with the Privacy Commissioner's office to help confirm ongoing compliance.

10.4 Judicial remedies

In addition to the quasi-criminal offences outlined above, which are prosecuted before the courts, PIPEDA allows both complainants and the Federal Commissioner, in some circumstances, to have the complaint heard on a *de novo* basis by the Federal Court, which may award damages or make other remedial measures. Such a hearing is only available once the matter has been investigated by the Commissioner and a finding made.

However, no damages had actually been awarded until this year, when three modest damage awards were made (see section 10.6 below), apparently stemming more from a desire by the Court to deter non-compliant behaviour, rather than to compensate for actual damages incurred (although the statute explicitly indicates that the Court may award damages for any humiliation that a complainant may have suffered).

10.5 Class actions

There has been little, if any, successful class action litigation in Canada respecting statutory privacy damages, although suits tend to be initiated after all major reported breaches. There may be several reasons for this, including the fact that thus far, the breaches in Canada do not appear to have led to any material personal damages, the fact that few of the statutes create a private right of action (only the Alberta and BC laws have them), the fact that such a right of action only arises after a full investigation and adjudication from the relevant Privacy Commissioner, and the fact that class action litigation is required to be certified in Canada, creating somewhat of a hurdle to such suits.

10.6 Liability

Individuals can sue organisations for damages stemming from non-compliance with the Alberta and BC private sector Acts, and in fact, it is only such individuals who have a right to damages under these statutes. As noted above, there have been three successful applications for damages before the Federal Court, however each resulted in a damage award of less than $5,000. It is perhaps in part because of the low financial sanctions levied against non-compliant companies that several of the Privacy Commissioners are lobbying for legislative amendments that would give them the power to directly impose administrative monetary penalties, as some other agencies can do.

Cyprus

Andreas Neocleous & Co LLC
Nicholas Ktenas & Chrystalla Neophytou

1. LEGISLATION

1.1 Name/title of the law

The Processing of Personal Data (Protection of Individuals) Law of 2001 (the Law) came into force on 23 November 2001. The Law was introduced in the context of harmonisation with the European Data Protection legislation and amended in 2003 in order to align domestic legislation with Directive 95/46/EC of the European Parliament and the Council Decision 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.

Furthermore, the Constitution of the Republic of Cyprus, which was established in July 1960, provides for the following two provisions regarding privacy:

- Article 15 states that every person has the right to respect for his private and family life and that there shall be no interference with the exercise of this right, except such as is in accordance with the law and is necessary in the interests of the security of the Republic, constitutional order, public safety, public order, public health, public morals or the protection of the rights and liberties guaranteed by the Constitution to any person.
- Article 17 of the Constitution provides that every person has the right to respect for, and to the secrecy of, his correspondence and other communication, if such other communication is made through means not prohibited by law.

1.2 Pending legislation

On 15 September 2011 the Ministry of Interior submitted a proposed amendment to section 5 of the Law, which sets out the grounds for legitimate processing, to be considered by the Committee on Financial and Budgetary Affairs. The amendment provides that the processing of data without the consent of the data subjects is legitimate if it is necessary for state security; the defence of the state; public security; the prevention, examination, investigation and prosecution of breaches of criminal law or the code of conduct of the legally established professions; and to safeguard important economic and financial interests of a member state or the EU, including monetary, fiscal and tax issues. The discussion is at a very early stage and the opinions of the Cyprus data protection authority, the Office of the Commissioner for the Protection of Personal Data (Commissioner) or other interested parties have not yet been submitted to the House of

Representatives.

1.3 Scope of the law

1.3.1 The main players

- A 'data controller' is any person who determines the purpose and means of the processing of personal data.
- A 'data processor' is any person who processes personal data on behalf of the controller. Acting on behalf of someone means serving someone else's interests and recalls the legal concept of 'delegation'. In the case of data protection law, a processor is called to implement the instructions given by the data controller at least with regard to the purpose of the processing and the essential elements of the means.
- A 'data subject' is a natural person to whom the data refer and whose identity is known or can be directly or indirectly ascertained, in particular on the basis of his identity number or on the basis of one or more relevant elements which characterise his existence from a physical, biological, psychological, economic, cultural, political or social point of view.
- A 'third party' is any person other than the data subject, the data controller and the data processor and the persons who, under the direct supervision or on behalf of the controller, are authorised to process the personal data.

1.3.2 Types of data

'Personal data' or merely 'data' are defined under section 2 of the Law as 'all information which refers to a living data subject'. Anonymous data are not considered to be personal data.

According to the Commissioner, a simple email address, even though it may not disclose its owner's identity, as well as the online habits of a person that can create his profile, can constitute personal data.

'Sensitive data' are data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, participation in a union, club or trade union organisation, health, sexual life and sexual orientation, as well as anything relevant to criminal prosecutions or sentencing.

1.3.3 Types of acts/operations

The law applies to the processing of personal data wholly or partly by automated means, and to the processing by other means of personal data which form part of a filing system (any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis) or which are intended to form part of a filing system.

1.3.4 Exceptions

The Law does not apply to the processing of personal data performed by a natural person in the course of a purely personal or a household activity.

1.3.5 Geographical scope of application

The Law applies to any processing of personal data which is performed:

- by a controller established in the Republic of Cyprus or in place where Cyprus law applies by virtue of public or international law; or
- by a controller not established in the Republic of Cyprus who, for the purposes of the processing of personal data, makes use of means, automated or otherwise, situated in the Republic of Cyprus, unless such means are used for the purposes of transmission of data through the Republic of Cyprus. In such a case the controller must designate, by a written statement submitted to the Commissioner, a representative established in the Republic of Cyprus, who is vested with the rights and undertakes the obligations of the data controller, the latter not being discharged from any special liability.

2. DATA PROTECTION AUTHORITY

The Office of the Commissioner for the Protection of Personal Data
(*Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*)
Iasonos 1, 2nd floor 1082, Nicosia, Cyprus
P.O Box 23378
T: +357 22818456
F: +357 22304565
E: commissioner@dataprotection.gov.cy
Web: *www.dataprotection.gov.cy*

2.1 Role and tasks

The Commissioner is a public independent administrative authority and its primary objective is to apply the Law and to ensure that every individual's right to privacy is protected when personal data are processed.

2.2 Powers

The Commissioner has the following powers:

- to inspect and supervise data controllers on its own initiative or following a complaint;
- to issue recommendations and opinions;
- to provide information and guidelines to the public as to their rights and obligations under the Law;
- to impose administrative fines on data controllers if found in breach of the Law; and
- to authorise upon application various processing activities that comply with the Law.

2.3 Priorities

No specific priorities have been set by the Commissioner; rather its focus is on the application of the Law and compliance of all relevant parties with it.

3. LEGAL BASIS FOR DATA PROCESSING

Section 5 of the Law specifies that personal data may be processed only if the

data subject has unambiguously given his consent. Non-sensitive personal data may be processed without the data subject's consent for certain specified reasons.

On the Commissioner's recommendation the Council of Ministers may make special rules for the processing of the most common categories of processing and filing systems or where serious matters of public interest make it appropriate. No such rules have yet been published.

3.1 Consent

3.1.1 Definition

Consent of the data subject is defined as any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject, having been previously informed, consents to the processing of personal data concerning him. The Commissioner has also adopted the Article 29 Data Protection Working Party's Opinion on Consent (WP 187).

3.1.2 Form

In principle the Commissioner does not require consent to be given in a specific form.

Sensitive personal data may be processed provided that the data subject has given his explicit consent. However, if the consent of the data subject was obtained unlawfully or is contrary to morals, custom or a specific law, consent does not lift the prohibition.

3.1.3 In an employment relationship

Consent must be given freely. In an employment relationship it may be questioned whether the subordinate position of the employee allows consent to be truly 'free', but this question has not yet been tested in the courts.

3.2 Other legal grounds for data processing

Non-sensitive personal data may be processed without the data subject's consent for one or more of the following reasons:

- for compliance with a legal obligation to which the data controller is subject;
- for the performance of a contract to which the data subject is party, or in order to take measures at the data subject's request prior to entering into a contract;
- in order to protect the vital interests of the data subject;
- for the performance of a task carried out in the public interest or in the exercise of public authority vested in the data controller or a third party to whom the data are communicated;
- for the purposes of the legitimate interests pursued by the data controller or by the third party to whom the personal data are communicated, on condition that such interests override the rights, interests and fundamental freedoms of the data subjects concerned.

The collection and processing of sensitive data are generally prohibited by the Law and allowed only if the data subject has given his explicit consent or otherwise if at least one of the following conditions is fulfilled:

- processing is necessary in order for the data controller to fulfil his obligations or carry out his duties in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
- processing is carried out by a foundation, association or other not-for-profit organisation which has political, philosophical, religious or trade union aims, and the processing relates solely to its members and other persons with whom the organisation has relations in order to attain its objectives. Such data may be communicated to third parties only if the data subject gives his consent;
- the processing relates solely to data which are made public by the data subject or are necessary for the establishment, exercise or defence of legal claims before the court;
- the data are medical data and processing is performed by a person providing health services by profession who has a duty of confidentiality or is subject to relevant codes of conduct, on condition that the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or the management of healthcare services;
- processing is necessary for the purposes of national security or criminal policy, and is performed by a service of the Republic of Cyprus or an organisation or foundation authorised for this purpose by a service of the Republic and relates to the detection of crimes, criminal convictions, security measures and investigation of potential terrorist offences;
- processing is performed solely for statistical, research, scientific and historical purposes, and all appropriate measures are taken for the protection of the data subjects; or
- processing is performed for journalistic purposes or in the framework of artistic expression as long as the right to privacy and family life is not violated.

With regard to employees' sensitive personal data, section 11 of the Employment Order issued by the Commissioner provides that the employer may maintain data concerning the previous convictions of the employee, such as traffic accidents committed by a professional driver. It also provides that the collection and processing of such data must be absolutely necessary for purposes connected to the employment relationship or where this is imposed by national legislation. Where the collection of such data is deemed necessary, employers must inform employees in advance of the purpose. In any event, the data collection must also be in accordance with section 10 of the Police Law (Law 73(I)/2004), which, *inter alia*, provides that the Head of Police shall issue a certificate concerning the employee's clean record stating any sentencing only following an application made by the employee/applicant or his duly authorised representative (eg, employer).

The Law empowers the Council of Ministers to issue regulations providing for the processing of sensitive personal data in cases other than those mentioned above, when there are important reasons of public interest. No such regulation has been issued to date.

3.3 Direct marketing and cookies

The Law specifies that personal data cannot be processed by anyone for the purposes of direct marketing or provision of such services, unless the data subject notifies his consent to the Commissioner in writing. The Commissioner keeps a register with the details of the identity of all these persons. The data controller must therefore consult the register before each processing and record in its filing system the persons included in the register.

The use of techniques such as the collection of cookies, web-bugs (files designed to trace web-visitors) or other technical methods that are not always obvious to the data subjects concerned and which allow website operators to create detailed profiles of visitors, according to their preferences and visits to web pages, third party advertisements and the like, is not essentially incompatible with the Law. However in order to make the use of such techniques legitimate, the website operator should always inform visitors of the intended use of their personal data and obtain their consent in relation to such use ('opt-in').

Directive 2002/58 on Privacy and Electronic Communications (the e-Privacy Directive) was transposed into national law in April 2004 in the Regulation of Electronic Communications and Postal Services Law of 2004, Law 112(I)/2004. The amendment to the e-Privacy Directive (Directive 2009/136/EC) has not yet been transposed into domestic law and no timetable has been announced for transposition. The Commissioner follows the guidelines set out in the Opinion of the Article 29 Data Protection Working Party on online behavioural advertising (WP 171).

3.4 Data quality requirements

Data controllers must ensure the fair and lawful processing of personal data. Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

Moreover, any personal data which are processed must be accurate, relevant and not excessive in relation to the purposes for which they are collected.

3.5 Outsourcing

The data controller may outsource the processing to a data processor. The data processor must possess appropriate qualifications and provide sufficient guarantees as regards technical knowledge and personal integrity for the protection of confidentiality. Regarding this issue, the Commissioner follows the principles set out in Opinion 3/2009 of the Article 29 Data Protection Working Party on the Draft Commission Decision on standard contractual

clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor).

3.6 Email, internet and video monitoring

3.6.1 General rules

The individual's right to private life and privacy of communications is established under the Constitution (in Articles 15 and 17 respectively) as well as in Article 8 of the European Convention of Human Rights. The Law for the Protection of the Confidentiality of Private Communications (Surveillance of Telecommunications) of 1996 (Law 92(I)/1996) gives effect to Article 17 of the Constitution. It requires the Attorney General to obtain a court order before monitoring private communications. In 2006 an amendment to Article 17 of the Constitution empowered the Attorney General to authorise telephone tapping under certain conditions, and the police to monitor web logs, downloads and emails as admissible evidence for criminal investigations.

The monitoring of emails and internet use, including monitoring by employers, is subject to the provisions of the Law, which does, however, not contain any specific provisions in this respect. The Commissioner has also issued general guidelines to raise public awareness regarding the dangers and risks relating to personal data and use of the internet. The purpose of these guidelines was to enlighten the general public as to the issues of identity theft, spyware, spam emails and phishing, and the particular issues involved in blogging and of social networking.

Video surveillance is also subject to the general provisions of the Law and the Commissioner has issued a Directive on Video Surveillance to provide good practice guidance in relation to the application of the Law to this form of personal data processing.

The Directive distinguishes between two environments in which video surveillance may take place. The first is premises which are privately owned but are freely accessible to the public, such as banks, shops and football fields; the second is public places, such as roads and parks, where the public expects there to be greater respect for its private life.

The Directive recommends that, although not legally obliged to do so, people who are responsible for the operation of CCTV should consult with the Commissioner before installing their systems, and follow any guidance given by the Commissioner.

According to the Directive, operators of CCTV systems which record natural persons must be in a position to justify their action as if they were collecting any other personal data.

By the very nature of CCTV, obtaining the express consent of data subjects as a legal ground for the data processing is highly impractical. However, if CCTV is used for the purposes of fighting, identifying and investigating crime, prosecuting criminal offences, public safety, protection of premises, national defence or security, road traffic monitoring and the like, the data controller will usually be in a position to invoke one of the other legal grounds for data processing (see section 3.2 above).

The use of CCTV in private premises can usually be justified by the owners on the grounds of prevention or detection of crime, or protection of a legitimate interest such as the security of their property.

However, in order to justify monitoring in public places a more careful approach will be necessary. The persons responsible for the operation of CCTV systems in public places must be in a position to show that the monitoring is necessary and that the benefits outweigh any resulting harm to the rights, interests and basic freedoms of the persons concerned.

CCTV should be installed only where there is no other alternative, less intrusive method capable of achieving the same end at a comparable cost. In accordance with section 4 of the Law, images should only be retained for as long as necessary to achieve the purposes of the recording. The persons responsible for the operation of CCTV cameras should have in place a specific retention policy for the recording media and should be in a position to justify the reasons for the selected retention period.

The person responsible for the operation of a CCTV system must file a written notification with the Commissioner, in accordance with section 7 of the Law, unless it falls within one of the exemptions to the Law.

The persons who will be recorded must be informed about the recording and given the right to decline to enter the building or the public premises in which the recording takes place.

All appropriate technical and organisational measures should be taken to ensure the security and confidentiality of any recordings, which should be accessible only to those who really need to see them.

No third party should be given access to the media unless there is a legitimate reason. For example, where the public can assist in identifying a criminal or a victim then it may be permissible to give access to the media.

If the recording includes images of other persons, their characteristics must be disguised before the recording is shown to a data subject who has requested access to his data so as not to violate their rights.

Data subjects have the right to request that the recording concerning them is destroyed, not used or not shown, in part or in whole, where they believe that the recording has not been carried out in accordance with the Law.

3.6.2 Employment relationship

Employers must take all possible steps to distinguish between employees' work and personal activities and restrict any monitoring to those activities which relate to the performance of their duties. For instance, an employer can install a system to monitor websites visited by his employees and their emails to ensure that use of the internet is made for work-related and not personal reasons. However, an employer is not allowed to access personal emails of employees in any event but should instead inform his employees that use of the email for reasons which are not work-related from computers which are installed at the workplace is not allowed and will be penalised.

In particular, employers have to respect the Law for the Protection of the Confidentiality of Private Communications (Surveillance of Telecommunications) of 1996 which prohibits interception or monitoring

of private communications of any kind, except with the previous express consent of both the originator and the recipient of the communication, or the consent of one of them in the case of indecent, annoying or threatening phone calls.

Monitoring of business emails, fax, internet websites, tracking phone calls, recording phone calls, CCTV monitoring and GPS monitoring are allowed under the Law as long as the employer can show that the monitoring is legitimate and necessary and that there are no other less intrusive means of achieving the intended objectives. These objectives must be such as to take priority over the rights, interests and fundamental freedoms of employees.

Voice recordings, pictures, email addresses and phone numbers of employees, which constitute personal data, if gathered through monitoring systems installed by an employer in the workplace, may only be used for the specific purposes for which they were gathered and must be destroyed or deleted after these purposes have been accomplished. For example, an employer who uses a CCTV system to monitor workplaces for security reasons may not use these systems for the purposes of monitoring employees during their breaks.

Before an employer installs any monitoring system he must first examine whether the intended control and monitoring as well as the data to be collected are proportionate to the purpose he seeks to accomplish. For example, it may not be necessary to monitor all employees or all of their activities and communications. The employer must choose the lowest level of monitoring necessary to meet the required objectives, with minimum possible intrusion into the personal life of employees.

The employer must inform his employees in advance about the purpose, the means and the duration of the control and monitoring to be applied. It is good practice for the employer to adopt a written policy which determines the parameters for employees' use of telephones, computers, internet and other similar facilities provided by the employer for their use and the ways in which the employer will control or monitor their use. Secret monitoring or monitoring without prior notice is prohibited under any circumstances.

Employers wishing to install monitoring systems in the workplace are recommended to consult employees or their trade union or other representatives to discuss the intended methods and consequences of monitoring. There is no obligation to consult.

Before providing a business with analytical statements with numbers dialled, telecommunications providers will require written confirmation that all users have been duly informed about the sending of such statements to the employer. Furthermore, unless the employer has received the express consent of the employees, the service provider must delete the last three digits from every number.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers are responsible for providing information to data subjects

regarding data relating to them.

4.2 What

The data controller must provide the following information to the data subject:

- the name and address of the data controller and his representative if any;
- the purpose of the data processing;
- the recipients or the categories of recipients of data
- the existence of the right of access and rectification of data;
- specific information that may be required based on the nature of the processing.

4.3 Exceptions

With the prior approval of the Commissioner, the data controller is exempt from providing information in the following circumstances:

- the data subject is already aware of the information;
- the processing is performed for statistical and historical purposes or for purposes of scientific research and it is impossible to inform the data subject;
- where disproportionate effort would be required in order to inform the data subject; or
- if the communication of data is provided by another law.

In addition, the Commissioner may wholly or partly exempt the data controller from the obligation to provide information if the collection of personal data is performed for the purposes of defence, national needs, or national security of the Republic of Cyprus or for the prevention, detection investigation and prosecution of criminal offences.

There is no obligation to inform where data are collected solely for journalistic purposes.

4.4 When

The Law provides that the data controller shall provide the information at the time of collection: that is, at the time when the data are recorded.

4.5 How

The Law provides that the information has to be given in an appropriate and an explicit way.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The Law provides that every person has the right to know whether the personal data relating to him are or were processed. This information must be given in writing.

Furthermore, at the request of a data subject, the data controller is required to provide, without excessive delay and expense, the following information:

- all the personal data relating to him which have undergone processing, the recipients or the categories of recipients as well as the categories of data which are or are to be processed;
- the purposes of the processing, the recipients or the categories of recipients, as well as the categories of data which are or are to be processed;
- the progress of the processing since any previous notification;
- the logical process upon which every automated processing of data in relation to the data subject is based, in cases where personal data are used to evaluate certain aspects of the data subject's personality.

In relation to health data, the data controller has the discretion to choose to give indirect access to the personal data. In that case, a healthcare professional will have access to the data and will report to the data subject.

To exercise the right of access, the data subject must submit a signed and dated request to the data controller, accompanied by proof of identity. The request may be sent by any appropriate means of communication.

5.1.2 Exceptions

See section 4.3 above.

5.1.3 Deadline

The data controller must communicate the information requested without delay, and at the very latest within four weeks after receipt of the request. If the controller does not reply within this period or if the data subject is not satisfied with the reply, the data subject has the right to appeal to the Commissioner.

5.1.4 Charges

The data subject may not be charged for exercising his right to access.

5.2 Rectification

5.2.1 Right

Any data subject has the right to require the data controller to rectify any incorrect personal data relating to him.

5.2.2 Exceptions

None.

5.2.3 Deadline

The data controller must rectify the personal data within four weeks of receiving the data subject's request.

5.2.4 Charges

A charge of €20 is payable by the data subject to the Commissioner.

5.3 Erasure

5.3.1 Right

Any data subject has the right to require the erasure of all personal data relating to him if the data are incomplete or irrelevant with a view to the purpose of the processing, if the recording, disclosure or storage of the data is prohibited, or if the data have been stored for longer than necessary.

5.3.2 Exceptions
See section 4.3 above.

5.3.3 Deadline
The data controller must erase the personal data within four weeks starting from the submission of the data subject's request.

5.3.4 Charges
None.

5.4 Blocking
5.4.1 Right
Any data subject has the right to block any use of personal data relating to him under the same conditions as the right to erasure.

5.4.2 Exceptions
See section 4.3 above.

5.4.3 Deadline
The data controller must erase the personal data within four weeks of receiving the data subject's request.

5.4.4 Charges
None.

5.5 Objection
5.5.1 Right
The data subject has the right to object, at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him.

5.5.2 Exceptions
None.

5.5.3 Deadline
The data controller must respond within four weeks of receiving the data subject's request.

5.5.4 Charges
The data subject will be charged €20 to exercise his or her right of access.

5.6 Automated individual decisions

5.6.1 Right

A decision producing legal effects for a data subject, or materially affecting him, cannot be taken purely on the basis of automated data processing aimed at evaluating certain aspects of his personality.

In the case of such an automated decision, the data subject has the right to be informed about the logic involved in any automated processing of data related to him.

5.6.2 Exceptions

The Law does not provide for any exceptions.

5.6.3 Deadline

There is no deadline.

5.6.4 Charges

The data subject may not be charged for exercising this right.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

Data controllers must notify the Commissioner in writing about the establishment and operation of a filing system or the commencement of processing. Responsibility for notification lies with the data controller.

6.1.2 What

Any type of automated or semi-automated (and in some cases manual) processing must be notified to the Commissioner.

6.1.3 Exceptions

The controller is discharged from the obligation to notify in the following circumstances:

- Processing is performed solely for purposes directly connected with the work to be done and is necessary for the fulfilment of a legal obligation or the performance of a contract, and the data subject has been previously informed.
- The processing concerns customers or suppliers of the data subject and the data are neither transferred nor communicated to third parties.
- Processing is performed by a society, association, company, political party or similar body and concerns data related to their members, who have given their prior consent, and the data are neither transferred nor communicated to third parties.
- Processing is performed by doctors or other persons who provide health services and concerns medical data, provided that the data controller is bound by medical confidentiality or any other kind of confidentiality required by law or code of conduct, and the data are neither transferred

nor communicated to third parties.
- Processing is performed by advocates and concerns the provision of legal services to their clients, provided that the data controller is bound by confidentiality required by law and the data are neither transmitted nor communicated to third parties, except in cases where it is necessary and directly connected with a request from the client concerned.

6.1.4 When
The Law does not specify when notification has to be made, but it is generally accepted that notification must be made prior to starting any automated processing activity.

6.1.5 How
The data controller is required to complete a paper copy of the standard notification form in Greek and submit it, together with the relevant fee, to the Commissioner. The standard notification forms are available on the website of the Commissioner. They include:
- the name and address of the controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description of the measures taken to ensure security of processing, in sufficient detail to allow a preliminary assessment to be made of their appropriateness and adequacy.

The Commissioner may require the notifying data controller to provide further information, for instance, regarding the origin of the personal data, the choice of automation technology and the security measures that are in place.

6.1.6 Notification fees
The notification fee is €50.

6.2 Authorisation requirements
6.2.1 Who
No authorisation is required to begin processing personal data. However, data controllers must obtain authorisation for data transfers.

6.2.2 What
Authorisation is required for the transfer of personal data to a country outside the European Economic Area (EEA).

6.2.3 Exceptions
None.

6.2.4 When

No transfer can be made until the application has been approved. Therefore the application must be made in good time. Periodic renewal is not required.

6.2.5 How

The data controller is required to complete a paper copy of the standard notification form in Greek and submit it to the Commissioner accompanied by any relevant documents such as consents, proof of the US 'safe harbour' registration, binding corporate rules or standard contractual clauses and the relevant fee. The requisite forms are available on the website of the Data Protection Commissioner.

6.2.6 Authorisation fees

The authorisation fee is €50.

6.3 Other registration requirements

Section 8 of the Law requires combinations of filing systems to be notified to the Commissioner by a statement submitted jointly by the controllers or by the controller who will combine two or more filing systems which are established for different purposes. 'Combination' means a form of processing which involves the possibility of connection of the data of one filing system with the data of a filing system or systems kept by another controller or other controllers or kept by the same controller for another purpose.

6.4 Register

The Commissioner maintains the following registers under the Law:

- a register of filing systems and processing notified to the Commissioner;
- a register of statements and authorisations issued by the Commissioner for the combination of filing systems;
- a register of persons not wishing to be included in filing systems which promote direct marketing or provision of services;
- a register of authorisations issued for the international transfer of personal data;
- a register of confidential filing systems, namely those systems maintained by the Ministers of Justice and Public Order and Defence and the Public Information Office, for the purposes of national security or the detection of particularly serious crimes. Combinations with at least one of these filing systems must also be registered in the register of Confidential Filing Systems.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

This role is not recognised under the Law and this is not a common role in Cyprus.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The transfer or 'transmission' of personal data in itself is an activity which falls within the definition of 'processing of personal data' as provided under section 2 of the Law.

Under section 9 of the Law the transfer of processed data or of data which will be processed when they are transferred to another country outside the EEA may take place only on the basis of an authorisation issued by the Commissioner, who will issue an authorisation only if he is satisfied that the country concerned ensures a sufficient level of protection.

8.2 Legal basis for international data transfers

Personal data may, with the Commissioner's prior approval, be transferred on the basis of satisfactory data transfer agreements or binding corporate rules or under the US 'safe harbour' scheme.

8.2.1 Data transfer agreements

There is a general obligation under Law 138(1)/2001 for the data controller to notify the Commissioner in writing about international transfers of personal data.

The data controller is discharged from the obligation to submit a notification to the Commissioner in cases where a transfer is performed solely for purposes directly connected with the work to be done and is necessary for the fulfilment of a legal obligation or for the performance of a contract, provided that the data subject has been previously informed. However, this does not apply to insurance companies, pharmaceutical companies, data provider companies such as providers of financial and stock market information and financial institutions, such as banks and credit card issuers.

8.2.2 Standard contractual clauses

The Commissioner will issue an authorisation if he is satisfied that the contractual arrangements between the data exporter and the third country recipient satisfactorily ensure the protection of private life and fundamental rights of the data subjects. This is typically achieved by using the 'standard contractual clauses' approved by the European Commission. Draft contracts, including those based on the standard contractual clauses, must be submitted to the Commissioner for approval. It should be noted that the standard contractual clauses are not necessary if the proposed transfer is to a recipient in a country that has been recognised by the European Commission as providing adequate protection of data.

8.2.3 Binding corporate rules

Binding corporate rules (BCRs) are internal rules adopted by multinational groups to define the group's global policy with regard to international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. Draft rules must be submitted to the Commissioner for approval together with a completed application form (available on the Commissioner's website). Cyprus participates in the mutual recognition procedure launched in

October 2008 by the Article 29 Working Party.

8.2.4 Safe Harbour

Data export may be authorised if the proposed data recipient is based in the US and participates in the 'safe harbour' self-certification scheme. However, participation is only one of the parameters considered by the Commissioner.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The Law provides that the processing of data is confidential and that it may be carried out only by persons acting under the authority of the data controller or the data processor and only upon instructions from the data controller.

In cases where the data controller delegates the processing to others, the data controller must select data processors who possess appropriate qualifications and who provide sufficient guarantees as regards technical knowledge and personal integrity so as to ensure that confidentiality of the data will be maintained.

9.2 Security requirements

The Law provides that the data controller must take the appropriate organisational and technical measures for the security of data and their protection against accidental and unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures must provide a level of security which is appropriate to the risks involved in the processing and the nature of the data processed.

9.3 Data security breach notification obligation

There is no obligation under Cyprus law to notify personal data security breaches to the data subjects concerned or to the Commissioner. Furthermore, the Commissioner has not issued any recommendation on this matter to date.

9.4 Data protection impact assessments and audits

There is no legal obligation under Cyprus law to carry out data protection impact assessments and audits.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Commissioner may adopt and issue opinions and make recommendations on his own initiative on any matter relating to the application of the fundamental principles of the protection of privacy and personal data.

The Commissioner can also issue an opinion on the merits of a complaint, which may contain recommendations for the controller. Furthermore either on his own initiative or in response to a complaint, the Commissioner may conduct an administrative inquiry into any filing

system. For this purpose the Commissioner has the right of access to personal data and to collect any requisite information, with only a few, limited exceptions.

10.2 Sanctions

In case of breach of the Law the Commissioner may impose the following administrative sanctions:

- a warning with a specific time-limit for rectification of the contravention;
- a fine of up to €10,000;
- temporary revocation of an authorisation;
- the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

Fines imposed by the Commissioner may be collected as a civil debt.

Contravention of the Law by a person responsible for processing, with intent to obtain an unlawful financial benefit for the perpetrator or anyone else, or to cause injury to a third party, is punishable on conviction by imprisonment for up to five years, a fine of up to €10,000 or both. The same sanction applies if the breach of the Law endangers the free functioning of the government of the Republic of Cyprus or national security.

The Data Protection Commissioner does not issue reports on enforcement actions or penalties.

10.3 Examples of recent enforcement of data protection rules

The Data Protection Commissioner's website gives details of complaints received and how they were dealt with. For the first half of 2011 details regarding four complaints have been published. In one of the cases, relating to the transfer of information on court judgments to a credit information bureau, the Commissioner found no breach of the law. In a case regarding the recording of telephone conversations by an insurance company the Commissioner ordered the company to make clear from the outset that calls would be recorded. The third case related to loss of medical records in a state hospital. The Commissioner found that there had been a breach of the requirement to take appropriate measures to safeguard data under section 10(3) of the Law and imposed an administrative fine of €1,500, taking into account that the hospital concerned had no record of previous breaches. The final complaint, regarding a social networking site, was transferred to the UK authorities when the site owner relocated there.

The largest fine imposed by the Commissioner to date is €8,000. This was in respect of a case in 2009 involving the sending of unsolicited text messages. The large number of complaints received, the fact that the sender did not cooperate and that he had previously been fined in respect of similar breaches were all taken into account in setting the fine.

10.4 Judicial remedies

Every person has the right to apply to the competent court for the immediate suspension or non-performance of an act or decision affecting

him, which has been done or made by an administrative authority or a public or private corporate body, a union of persons or a natural person by processing of data, where such processing aims to evaluate certain personal aspects relating to him and in particular, his efficiency at work, his financial solvency, his credibility and his behaviour in general. Action may be taken under the Courts of Justice Law, the Civil Procedure Law or any other law which provides for the issue of provisional orders.

Moreover, a person suffering any harm as a consequence of acts infringing the provisions of the Law can initiate a civil action for damages. There is no published case law, because such cases (if any) would be dealt with in the district courts, the decisions of which are not routinely reported.

10.5 Class actions

Class actions are not permitted under Cyprus law.

10.6 Liability

Data controllers are liable for any damage resulting from breaches of the Law. Data subjects that have incurred damage from an action in violation of the Law may claim damages from the data controller. The controller will not be liable if he proves that the act which caused the damage cannot be assigned to him.

Czech Republic

Havel, Holásek & Partners Richard Otevřel

1. LEGISLATION

1.1 Name/title of the law

In addition to international instruments protecting privacy and personal data, such as the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, the basis for privacy protection in the Czech Republic is provided for in the 1993 Charter of Fundamental Rights and Basic Freedoms (*Listina základních práv a svobod*), which constitutes the essential part of the constitutional core of the Czech legal system.

In this context, Act No. 101/2000 Coll., on Personal Data Protection of 4 April 2000 (*zákon o ochraně osobních údajů*), as amended (the Act), serves as the implementing norm, both in relation to the aforementioned constitutional freedoms and to the 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 (the Directive). The Act provides for a general legal framework for the protection of personal data and any other laws and regulations qualify as exemptions from it, or provide for a special regime concerning particular types of personal data and the means of processing them.

The following legislative acts form part of the overall system of data protection:

- Act on Electronic Communications of 1 May 2005 (*zákon o elektronických komunikacích*), as amended;
- Labour Code of 1 January 2007 (*zákoník práce*), as amended;
- Act on Healthcare of 1 July 1966 (*zákon o péči o zdraví lidu*), as amended;
- Act on Certain Information Society Services of 29 July 2004 (*zákon o některých službách informační společnosti*);
- Civil Code of 26 February 1964 (*občanský zákoník*); and
- Penal Code of 9 February 2009 (*trestní zákoník*).

1.2 Pending legislation

Currently, only bills concerning the Act on Electronic Communications are under discussion.

The first bill deals with the implementation of Directive 2009/136/EC, which has amended Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive) (for further details, see section 3.3 below). The bill is awaiting parliament's approval.

The second bill is a response to the Czech Constitutional Court's ruling

of March 2011 striking down the rules on data retention in the Act on Electronic Communications, which has implemented Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. The government is attempting to propose new balanced rules that enable law enforcement agencies to access both historical traffic and localisation data while at the same time ensuring an adequate level of protection of individual rights with regard to privacy in communication.

1.3 Scope of the law

1.3.1 The main players

- the 'data controller' means any entity that determines the purpose and means of data processing, carries out such processing and is responsible for such processing;
- the 'data processor' means any entity processing personal data pursuant to the Act, based either on a special law or on authorisation by a data controller;
- the 'data subject' means any natural person to whom the personal data pertain. A data subject shall be considered identified or identifiable if it is possible to identify the data subject directly or indirectly, in particular on the basis of a number, code, or one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity.

1.3.2 Types of data

The Act only covers personal data related to natural persons and not data related to legal persons (eg, companies).

'Personal data' are any information relating to an identified or identifiable data subject and include an individual's name, address, photograph, telephone number, bank account number, etc.

The Act distinguishes between two categories of personal data: apart from 'ordinary' personal data, 'sensitive data' are defined as personal data revealing nationality; racial or ethnic origin; political attitudes; trade union membership; religious and philosophical beliefs; conviction of a criminal act; health status; genetic information; and sexual life of the data subject, as well as any biometric data enabling the direct identification or authentication of the data subject. Sensitive data are subject to stricter processing conditions.

Personal data that have been made anonymous cannot be considered to be personal data, provided that such data cannot be linked to an identified or identifiable data subject. Any method that could wholly or partially enable the reconstruction of the link between the data and the data subject would not be considered as anonymisation, thus leaving such data to be considered personal data.

1.3.3 Types of acts/operations

The Act covers the 'processing' of personal data, defined as any operation or set of operations that is systematically executed by a data controller or a data processor in relation to personal data by automatic or other means. Processing shall mean, in particular, the collection of data, their storage on data carriers, and their disclosure, modification or alteration, retrieval, use, transfer, dissemination, publication, preservation, exchange, sorting or combination, blocking and liquidation.

The term 'systematically' is to be interpreted as being the opposite of accidental collection, unless these data are subject to further processing. Manual data processing is also covered by the Act insofar as the data forms part of a 'filing system' (eg, an 'analogue' index that enables the effective searching of the database for personal data).

1.3.4 Exceptions

Processing of personal data carried out by a natural person for personal needs exclusively falls outside the scope of the Act. As mentioned above, accidental collection that is not followed by any form of data processing is also exempt from the application of the Act.

Moreover, partial exemptions exist for the following types of data processing required by specific laws for securing:

(i) the security of the Czech Republic;
(ii) the defence of the Czech Republic;
(iii) public order and internal security;
(iv) the prevention, investigation, detection and prosecution of criminal offences;
(v) important economic interests of the Czech Republic or the European Union;
(vi) important financial interests of the Czech Republic or the European Union, in particular the stability of the financial market and currency, functioning of currency circulation, and system of payments, as well as budgetary and taxation measures; or
(vii) the exercise of control, supervision, surveillance, and regulation related to the exercise of public authority in the cases under (iii), (iv), (v), and (vi); or (viii) activities related to the disclosure of the files of the former State Security agency (*Státní bezpečnost)* (the 'exempted processing').

1.3.5 Geographical scope of application

The following two categories of data processing operations fall within the geographical scope of the application of the Act:

- The processing of personal data carried out in the context of the effective and actual activities of any data controller permanently established in the Czech territory, or in a place where Czech law applies by virtue of international public law.
- The processing of personal data by a data controller with no permanent establishment in the EU, if the processing occurs on Czech territory, unless the processing only consists of transiting through the EU. The data controller must designate a data processor as a representative to

carry out processing on Czech territory.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

The Office for the Protection of Personal Data (*Úřad pro ochranu osobních údajů*)
Pplk. Sochora 27, 170 00 Praha 7, Czech Republic
T: +420 234 665 555, +420 234 665 111
F: +420 234 665 444
E: posta@uoou.cz
W: www.uoou.cz

2.1 Role and tasks

The Office for the Protection of Personal Data (the Office) is an independent body and its primary objective is to ensure that every individual's right to privacy is protected when personal data are processed; however, over time the Office has acquired some further powers more or less related to the protection of personal data.

2.2 Powers

The Office has the following competences:

- performing supervision of the observance of the obligations provided by the Act;
- keeping a register of data processing;
- receiving complaints concerning the breach of the Act and providing information regarding their settlement;
- drawing up an annual report on its activities and making the report available to the general public;
- exercising other competences specified by law;
- dealing with cases of misdemeanours and other administrative offences and imposing fines pursuant to the Act;
- ensuring the fulfilment of requirements following from international treaties that bind the Czech Republic;
- carrying out consultations in the area of personal data protection; and
- co-operating with similar authorities in other countries, with institutions of the European Union, and with bodies of international organisations operating in the area of personal data protection. In accordance with the law of the European Communities, the Office is responsible for notifying the institutions of the European Union.

The most significant power is that the Office may carry out on-site investigations and request all necessary information, which the data controller, data processor or any other relevant person is obliged to provide. For measures and penalties imposed by the Office, see section 10 below.

2.3 Priorities

Every year, the Office adopts an annual report summarising the conducted investigations and drawing conclusions on the state of data processing in the Czech Republic, pointing out trends in this area, and outlining the priorities for the upcoming year.

The primary goals for 2011 remained mostly the same as in 2010: the use of video surveillance systems and processing biometric data (including genetic information). Additionally, the Office focuses on loyalty bonus programmes, including in the area of healthcare. Intensive educational programmes aimed at children (in cooperation with schools) are also still on the agenda.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Consent constitutes the principal legal basis for the processing of personal data. Although the data subject's consent is not defined in the Act, the Office has derived, from the related provisions and obligations of data controllers/data processors and the opinions of the Article 29 Working Party, the theory of informed consent, which has to be '*freely given, serious, specific, comprehensible and informed*'.

A common area of malpractice usually concerns the lack of information on data processing which would provide the whole picture of the processing (ie, who, why, what, and for how long). Moreover, the interpretation of the requirement that the consent should be given freely causes problems, especially in situations where no obvious alternative (following the refusal of consent) is available.

3.1.2 Form

The Act does not require any specific form, but the ability to prove that consent is given. Therefore, written consent is the most common form, together with the electronic tick-box method used on the internet. In appropriate situations, implied consent is also acceptable.

However, in the case of sensitive data, express consent is required, and therefore implied consent will not be sufficient.

3.1.3 In an employment relationship

Most personal data processed within the employment relationship may be processed without consent (see below section 3.2). In addition, the Labour Code provides for a limit on the extent of employee personal data that the employer may process. The employer may only request such data that directly relate to the work position of the particular employee. Acquiring (even indirectly) information on pregnancy; family and property situation; sexual orientation; origin; labour union membership; political or religious affiliation; or criminal conviction is expressly prohibited. However, information on pregnancy; family and property situation; and criminal convictions may be appropriately processed if it is substantiated by the nature of the work position, or if it is prescribed by law (for example, the

protection of pregnant women in certain professions, and the protection of economic/financial interests).

As far as other personal data are concerned, these should be provided to the employer only on a voluntary basis (eg, data necessary for employee participation in bonus programmes).

3.2 Other legal grounds for data processing

As an exemption from obtaining consent, non-sensitive personal data may be processed if one or more of the following conditions are met:

- if the data controller carries out processing which is essential to comply with his/her legal obligations;
- if the processing is essential for the fulfilment of a contract to which the data subject is a contracting party, or for negotiations on the conclusion or alteration of a contract suggested by the data subject;
- if it is essential for the protection of vitally important interests of the data subject. In this case, the consent of the data subject must be obtained without undue delay after the processing commences. If the consent is not granted, the data controller must terminate the processing and delete the data;
- in relation to personal data that were lawfully published in accordance with special legislation. However, this shall not prejudice the right to the protection of the private and personal life of the data subject;
- if it is essential for the protection of rights and legitimate interests of the data controller, recipient or other person concerned. However, such data processing may not contradict the data subject's right to protection of his private and personal life;
- if the data controller provides personal data on a publicly active person, official, or employee of public administration that reveals information on their public or administrative activity, their functional or working position; or
- if the processing relates exclusively to archive purposes, pursuant to a special law on archiving.

Processing of sensitive data may be carried out without the data subject's consent only if one or more of the following conditions are met:

- if it is necessary in order to preserve the life or health of the data subject or some other person, or to eliminate imminent serious danger to their property, if his consent cannot be obtained, in particular, due to a physical, mental, or legal incapacity, or if the data subject is missing. The data controller shall be obliged to terminate the data processing as soon as the abovementioned reasons cease to exist, and must delete the data, unless the data subject gives his consent to continuation of the processing;
- if the processing in question is in relation to ensuring health care, public health protection, health insurance, and the exercise of public administration in the field of the health sector, pursuant to a special law, or if it is related to the assessment of health in other cases provided by a special law (such as the Act on Healthcare);

- if the processing is necessary to keep the obligations and rights of the data controller responsible for processing in the areas of labour law and employment provided by a special law;
- if the processing pursues political, philosophical, religious, or trade union aims and is carried out within the scope of a legitimate activity of a civil association, foundation, or other legal person of a non-profit nature ('the association'), and which only relates to members of the association or persons with whom the association is in recurrent contact related to the legitimate activity of the association, and the personal data are not disclosed without the consent of the data subject;
- if the data processed pursuant to a special law are necessary to administer health insurance, social insurance (security), state social support, and other state social benefits, social care, and the social and legal protection of children, and if, at the same time, the protection of these data is in accordance with the law;
- if the processing concerns personal data published by the data subject;
- if the processing is necessary to secure and exercise legal claims;
- if the processing exclusively relates to archive purposes pursuant to a special law on archiving; or
- if the processing exclusively relates to special activities conducted for the prevention, search, and detection of criminal activities, their prosecution, and searching for persons.

Processing of health data is specifically regulated in the Act on Healthcare, where access to health data (for healthcare practitioners and the data subjects' relatives) and its retention is particularly provided for.

3.3 Direct marketing and cookies

The Act only provides for partial regulation of direct marketing, but it still creates a substantive deviation from the general rules on protection of personal data. In particular, if the data controller or the data processor execute data processing for the purpose of offering business opportunities or services to the data subject, only a limited scope of personal data (name, surname, and address) may be used for this purpose, provided that the data were: (i) acquired from a public record; or (ii) acquired in the context of the activities of the data controller or the data processor (ie, usually obtained from the data subject directly or from an authorised third party).

The data controller must always cease processing such data if the data subject expresses his/her objection (so-called 'opt-out'). If the data subject has opted-out, a data controller is entitled (and in fact it is advisable to do so) to continue processing the data containing the name, surname, and address of the data subject only for the purpose of keeping a blacklist of opted-out persons.

Moreover, it is prohibited to cross-reference any other personal data to the name, surname, and address without the consent of the data subject.

Such data may be forwarded by one data controller to another (but the second data controller cannot transfer it to any other person without consent) provided that:

- they were acquired in relation to the activities of the data controller or the data concerned are publicly available personal data (ie, from public sources);
- they will be used solely for the purpose of offering certain business opportunities or services to the data subject; and
- the data subject has been informed by the data controller prior to the transfer and has not objected to the transfer in writing – this warning may be provided as information during the process of collecting data, whereby such a process is usually used to obtain consent anyway.

In addition to the general rules mentioned above, the Act on Certain Information Society Services provides for an opt-in mechanism regarding the use of electronic contact details (ie, email address, telephone number, ICQ or Skype number, etc) (so-called 'opt-in'). In other words, no one may use electronic contact details for commercial communication without the previous consent of the data subject.

The use of cookies or equivalent devices is regulated by Article 89 of the Act on Electronic Communications, which implements Article 5(3) of the ePrivacy Directive (the cookie clause), and has enacted the opt-out principle. In other words, the use of cookies and equivalent devices is permitted only if: (i) the user or subscriber has been informed of the purposes of the data processing and of his rights; and (ii) the data controller has offered the user or subscriber the possibility of opting out before installing the cookies.

The currently proposed bill for implementing Directive 2009/136/EC of 25 November 2009, which amends, in particular, Article 5(3) of the ePrivacy Directive, and contains stricter rules on the use of cookies, seems to leave the opt-out regime as it is and it is therefore questionable whether it would constitute a correct implementation of the cookie clause. However, the cookie clause was only a marginal issue in the proposed bill, so no public discussion concerning the interpretation of Article 5(3) of the ePrivacy Directive has so far occurred in the Czech Republic.

3.4 Data quality requirements

Data controllers must ensure that only accurate data obtained in accordance with the Act (for specified, explicit, and legitimate purposes, and only to the extent required for such purposes) are collected and processed. If the personal data are inaccurate with regard to the purpose for which they were collected, the data controller must immediately take the appropriate measures to update, amend or even block the personal data. In addition, the information showing that the data are inaccurate must also be provided to all the recipients of such data.

3.5 Outsourcing

When outsourcing data processing activities to data processors, the data controller is required to select a data processor to take the necessary security measures, supervise the data processor's compliance with these security measures, and enter into a written agreement with the data processor. The written agreement must:

- specify the scope and purpose of the data processing;
- specify the duration of the agreement; and
- stipulate the data processor's guarantees for the technical and organisational security measures.

Sub-contracting of the data processor's rights and obligations is not permitted by law; however, technical services may be provided on the basis of a special contract specifying exactly what kind of data and under what conditions such a subcontractor may access and process (ie, such a subcontractor does not acquire the status of a data processor).

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use and the use of surveillance cameras is not specifically regulated by the Act. The plan to expressly regulate the use of cameras by amending the Act has not yet been realised.

The Act on Electronic Communications imposes upon operators the obligation to ensure the protection of the communication, with the only exemption applying to law enforcement agencies under strict conditions provided in the Criminal Proceedings Act and other specific laws. Furthermore, in addition to electronic communications, regular mails and other information kept in secret by any individual are protected by the Penal Code.

The privacy of communication (other than electronic communication) and expression of personality are protected by the general provisions of the Charter for Fundamental Rights and Basic Freedoms. Any record (audio, photo, video, in writing) of a personal nature is basically excluded from unauthorised exploitation, unless a specific 'exemption' applies, such as for journalistic purposes, educational, scientific, and artistic activities.

Special laws enable the police to use video surveillance systems in public spaces and provide for brief rules on the protection of any records kept. Use of a video surveillance system in the private sector is usually founded upon the need to protect personal property, while the necessity and adequacy of this measure is strictly assessed by the Office during the notification of the system.

3.6.2 Employment relationship

According to the Labour Code, which contains the only guidance on this subject, an employer is entitled to adequately monitor in order to ensure that employees do not abuse their working tools (including IT and communication devices) for their own purposes. However, this right does not enable the employer to invade the employees' privacy, especially using open or covert monitoring, wiretapping, or searching mail and emails addressed to the employee.

The only exception from the ban on monitoring is a situation in which the employer may substantiate the monitoring using the 'specific activities of the employer', for example, if higher security is necessary (such as for hazardous operations or higher risk of criminal activity). The employees must be informed of such monitoring in advance.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers are responsible for informing the data subjects about the processing of personal data related to them.

4.2 What

Unless the data subject is already aware of this, the data controller must provide the following information to the data subject:

- the identity of the data controller, the data processor, and the recipient of the data, if any;
- the purpose(s) and extent of the data processing;
- the existence of the right to access the personal data;
- the existence of the right to the rectification of the personal data, as well as other rights (see section 5 below).

This obligation may be also fulfilled by the data processor.

The data controller is exempt from providing the above information if:

- he processes personal data exclusively for the purposes of a statistical service of the state, scientific, or archive purposes, and the provision of such information would involve a disproportionate effort or inadequately high costs, or if storage on the data carriers or disclosure is expressly provided by a special law. In these cases, the data controller is obliged to take all the necessary measures to protect against unauthorised interference with the data subject's private and personal life;
- the data processing is imposed by a special law, or such data are necessary to exercise the rights and obligations ensuing from special laws and regulations;
- he exclusively processes lawfully published personal data; or
- he processes personal data obtained with the consent of the data subject.

If the data have been obtained directly from the data subject, the data controller must also inform the data subject of whether the provision of the personal data is voluntary or mandatory. In the latter case, if such an obligation is prescribed by law, the data subject must be informed about the consequences of refusing to provide personal data.

4.3 When

The information should be provided at the time when the personal data are recorded. If the data are not directly obtained from the data subject, the information should be provided without any undue delay.

4.4 How

The Act does not specify in which form and how the information must be provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Upon request, every data subject has the right to know whether a certain

data controller is processing personal data on him and, if so, the categories of the personal data and the available information regarding their source, the purposes and methods of the processing, and the recipients, or the categories of recipients, to whom the data are disclosed.

The Act does not specify the form in which the above information should be provided (nor the form of the request), but the Office advises that a copy of the personal data concerned is provided so that the data subject may effectively exercise at least the related right of rectification.

For health-related data, the data subject may choose to grant access to his/her personal data to any third persons. The usual practice is to provide the list of authorised persons upon admission to the healthcare facility.

5.1.2 Exceptions

The right of access can, under no circumstances, be refused, unless provided for in special laws (especially the Criminal Proceedings Act, ensuring that law enforcement authorities' investigations are not hampered by an inappropriate request for information).

5.1.3 Deadline

The data subject can exercise the right to access at any time. In response, the data controller must communicate the information without delay.

5.1.4 Charges

The data subject may be charged for exercising his right to access only to the extent of the necessary costs involved in the provision of the information.

5.2 Rectification

5.2.1 Right

Any data subject has the right to obtain from the data controller the rectification of any incorrect personal data relating to him.

5.2.2 Exceptions

There are no exceptions to the right to rectification.

5.2.3 Deadline

If the data subject's request is justified, the data controller must rectify the personal data without delay.

5.2.4 Charges

The data subject may not be charged for exercising his right to rectification.

5.3 Erasure

5.3.1 Right

Any data subject has the right to obtain the erasure of all the personal data related to him if the data are incomplete or irrelevant, with a view to the purpose of the processing, or, generally, if the (further) processing is prohibited.

5.3.2 Exceptions
There are no exceptions to the right to erasure.

5.3.3 Deadline
If the data subject's request is justified, the data controller must erase the personal data without delay.

5.3.4 Charges
The data subject may not be charged for exercising his right to erasure.

5.4 Blocking
5.4.1 Right
Any data subject has the right to block any use of the personal data related to him, under the same conditions as the right to erasure/rectification.

5.4.2 Exceptions
There are no exceptions to the blocking right.

5.4.3 Deadline
If the data subject's request is justified, the data controller must block the personal data without delay.

5.4.4 Charges
The data subject may not be charged for exercising his blocking right.

5.5 Objection
5.5.1 Right
The Act does not provide for a specific right to object to data processing other than in the case of direct marketing (see section 3.3 above).

5.5.2 Exceptions
None.

5.5.3 Deadline
The processing must stop, without delay, upon objection.

5.5.4 Charges
The data subject may not be charged for exercising the right to object.

5.6 Automated individual decisions
5.6.1 Right
A decision producing legal effects for a data subject, or materially affecting him, cannot be taken purely on the basis of automated data processing aimed at evaluating certain aspects of his personality. The Act prescribes that any such decision, based exclusively on automatically processed data, must be reviewed before it is issued.

5.6.2 Exceptions
The right does not apply if the decision is beneficial for the data subject or is issued on his/her request.

5.6.3 Deadline
Not applicable.

5.6.4 Charges
Not applicable.

5.7 Other rights
5.7.1 Right
Any data subject has the right to request the Office to exercise its investigative powers where there is a possible breach of the Act by the data controller, data processor or any other person processing his/her data.

5.7.2 Exceptions
There are no exceptions.

5.7.3 Deadline
There is no deadline, although the real powers of the Office might be limited if the alleged breach occurred more than three years before the initiation of the administrative proceedings (investigation).

5.7.4 Charges
The data subject may not be charged for exercising this right.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The responsibility for notification to the Office lies with the data controller.

6.1.2 What
In principle, any data processing activity must be notified, unless statutory exemptions apply.

6.1.3 Exceptions
The data controller is exempt from notification if:
- the processing relates to personal data that are part of data files publicly accessible on the basis of a special law (such as data from the Commercial Register);
- the processing is imposed on the data controller by a special law or when such personal data are needed for exercising rights and obligations deriving from a special law (this exemption is quite usual, for example, in an employment relationship, when processing telecommunications data, etc); or
- in the case of processing that pursues political, philosophical, religious

or trade union aims carried out within the scope of legitimate activity of an association and which relates only to members of the association or persons with whom the association is in recurrent contact related to the legitimate activity of the association, and the personal data are not disclosed without the consent of data subject.

6.1.4 When

Notification must be made prior to commencing any processing activity (the data controller must wait until the Office registers the processing).

The Act does not impose an obligation to inform the Office of the termination of the processing. In reality the register kept by the Office contains many registrations that are no longer up-to-date, however, the Office may cancel the registration either upon the data controller's request or if the Office finds that the purpose of the registered processing ceased to be valid.

On the other hand, if the data controller winds up his activity, he must always inform the Office of how the personal data (for which processing was registered) will be handled thereafter (eg, if they are to be handed over to another data controller or destroyed).

6.1.5 How

Notification may be made online via the Office's website or by completing a hard copy notification form (available on the Office's website) and sending it back to the Office.

Unless the data controller so requests, the Office does not give information about the registration (the status of the registration may, however, be monitored on the Office's website). Once the notification is registered the data controller may start the notified processing activity, unless prior authorisation for data transfers abroad is required (see section 6.2 below).

Notification must be made in Czech.

Each purpose for which personal data are processed, or each group of connected purposes, requires a separate notification. The notification form includes information about the purpose of the processing; the name and address or registered office of the data controller and known data processors; the categories of the personal data processed; the receiving data controllers; information on international data transfers; and a basic description of the security measures.

The Office is entitled to demand additional information from the notifying data controller, for instance, demonstrating adequacy for processing sensitive data or appropriateness when installing video surveillance systems. Basically, the Office usually asks questions informally and once the requested information is provided, the registration continues. The Office has 30 days to finalise the registration from the day it received the completed notification – if the Office does not initiate administrative proceedings (due to serious doubts about the legality of the notified processing) and does not register the processing either, the processing is

deemed to be registered on the 30th day after notification.

In 2010, the Office received 4,037 notifications. This number includes modifications to existing notifications (906) and notifications regarding the termination of a processing activity (119).

6.1.6 Notification fees

There is no fee for the notification.

6.2 Authorisation requirements

In principle, data controllers do not need to obtain authorisation to carry out a data processing activity, but authorisation may be required for certain types of international data transfers (see section 8 below).

6.3 Other registration requirements

For registering video surveillance systems, additional information is required for notification: a detailed description of the purpose/reasons for the processing; the exact number of cameras; types of cameras (stationary/mobile) and their location; the monitoring regime (what time of day); how the monitored persons are made aware of the system; and the storage period of the video records. If the system is used for monitoring the workplace, it must also state how the protection of the employees' privacy and human dignity is ensured.

6.4 Register

The Commission holds a public register of notified processing operations, which may be consulted by anyone, free of charge, at *www.uoou.cz/uoou.aspx?menu=29&submenu=30&loc=503*. For each processing, the public register contains the same information as is provided in the notification form (however, it may be shortened by the Office).

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The Act does not recognise data protection officers.

7.2 Tasks and powers

Not applicable.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

No restrictions apply to data transfers to:

- EU member states;
- signatory states of the European Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108); or
- 'adequate countries' as officially recognised by the European Commission (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey and Switzerland).

For other countries, additional conditions must be fulfilled and/or the Office's approval sought (see section 8.2 below).

8.2 Legal basis for international data transfers

Data may be transferred to non-adequate third countries in two ways:

- by signing standard contractual clauses (as approved by the European Commission or by the Office; the Office has not yet approved its own clauses yet and relies on those of the European Commission); or
- by seeking the Office's authorisation together with proving that one or more of the following criteria are met:
    - the transfer is made with the consent or on instructions of the data subject;
    - adequate special safeguards for the protection of the personal data are provided in the country where the personal data will be processed. For example, such safeguards may be provided by means of other general or sectoral rules of law or professional rules and security measures. The safeguards may, in particular, be further specified in an agreement concluded between the data controller and the data recipient containing the appropriate contractual clauses (these are national, standard contractual clauses as opposed to standard contractual clauses published by the EU) or otherwise securing the protection of the transferred personal data;
    - the transfer involves personal data available in a public registry in accordance with a specific law;
    - the transfer is necessary for the purposes of an important public interest which is either in accordance with a specific law or an international treaty binding on the Czech Republic;
    - the transfer is necessary for negotiations concerning the execution or variation of an agreement initiated at the request of the data subject, or for the performance of an agreement to which the data subject is a party;
    - the transfer is necessary for the performance of an agreement concluded in the interest of the data subject between the data controller and a third party, or for the purposes of exercising another legal claim; or
    - the transfer is necessary for the protection of the rights or vitally important interests of the data subject (eg, the preservation of the life or health of the data subject).

Before granting the authorisation, the Office will examine the circumstances relating to the data transfer, including the source, destination, purpose, term and categories of the data, along with the available information concerning the level of protection of personal data in the recipient country. The authorisation will then specify the period during which the transfer is authorised.

8.2.1 Data transfer agreements

As mentioned above, the European Commission's standard contractual

clauses are the legal basis for 'safe' transfer itself, without the need for the Office's authorisation. Moreover, there is no requirement to present these agreements during the notification (if the processing is subject to notification) and, as a result, the use of these agreements is a common and easy way to achieve compliance with the rules regarding international data transfers.

The fact that the international data transfer is made pursuant to standard contractual clauses must be mentioned in the notification form.

8.2.2 Binding corporate rules

Binding corporate rules (BCRs) provide the required 'adequate special safeguards' (see section 8.2 above) but data transfers based on BCRs still require the Office's authorisation. There is no specific procedure available for the application of BCRs and there have been no practical examples yet.

8.2.3 Safe Harbour

There is no need for an authorisation if the personal data are transferred to an organisation that is certified under the US Safe Harbour scheme and the data transfer falls into the scope of that certification.

The fact that the data transfer is made to a US Safe Harbour certified organisation must be mentioned in the notification form (if the processing is subject to notification).

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The Act requires data controllers and data processors to ensure the confidentiality and security of personal data.

Confidentiality is primarily ensured by imposing such an obligation upon the data controller's employees and other persons accessing personal data (by virtue of either an agreement or a special law). The obligation of confidentiality survives beyond the employment relationship or termination of relevant works.

9.2 Security requirements

According to section 13 of the Act, both the data controller and the data processor are responsible for adopting appropriate measures to prevent any unauthorised or accidental access to personal data, alteration or other abuse of the personal data (even after terminating the data processing).

The data controller or the data processor must prepare and document the adopted and implemented technical and organisational measures for ensuring protection of personal data. To that end, the data controller or data processor conducts the relevant risk assessments concerning:

(i) performance of instructions related to data processing by persons having direct access to personal data;
(ii) prevention of unauthorised access to personal data and means for processing;
(iii) unauthorised reading, creating, copying, transfer, alteration or deletion

of personal data; and
(iv) measures enabling identification of to whom personal data were provided.

In addition, in the area of automatic processing systems, the data controller and the data processor are obliged to ensure that:
(i) the systems may be used only by authorised persons;
(ii) the authorised persons have only such access rights as are necessary;
(iii) there is electronic auditing enabling identification of who has accessed (or created) data, when and why; and
(iv) unlawful access to data carriers is restricted.

9.3 Data security breach notification obligation

There is no obligation under Czech law to notify personal data security breaches to the data subjects and/or to the Office.

In the proposed amendment to the Act on Electronic Communications (so only applicable to telecommunications services), new provisions would require that in the event of a data breach, the operator should inform the Office, and in the event of serious breaches, also the data subject.

9.4 Data protection impact assessments and audits

For general requirements on risk analysis, see section 9.2 above. Otherwise, no formal data protection impact assessments and audits are required by the Act.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Office may carry out targeted inspections on its own initiative or may investigate complaints it receives. The Office may carry out on-site investigations. In the course of the investigation, the data controller must provide all necessary information upon request and co-operate with the Office.

If the Office identifies any breach of the Act, remedial measures, including orders for the deletion of the personal data concerned, together with deadlines for compliance, are imposed. Among the possible measures, the deletion of data may be ordered. The data controller may appeal to the president of the Office (and subsequently to the administrative court, if he is still unsuccessful with his objections), but until the case is definitely resolved, the personal data must be blocked.

According to its 2010 Annual report, the Office initiated 106 audits of processing operations in 2010 and 163 inspections concerning unlawful direct marketing activities.

10.2 Sanctions

The processing of personal data in breach of the Act may constitute an administrative offence, penalised with fines of up to CZK 10 million and structured as follows:

- natural person for breaching confidentiality: up to CZK 100,000;

- natural person as a data controller: up to CZK 1 million;
- natural person endangering a larger number of persons by unlawful intrusion into privacy or breaching obligations concerning processing of sensitive data: up to CZK 5 million;
- legal person as a data controller: up to CZK 5 million; or
- legal person endangering a larger number of persons by unlawful intrusion into privacy or breaching obligations concerning processing of sensitive data: up to CZK 10 million.

In addition, natural persons are also subject to criminal penalties should they unlawfully disclose personal data in breach of their confidentiality obligations. The penalties include up to eight years of imprisonment in extreme cases. So far, criminal sanctions have not yet been imposed.

10.3 Examples of recent enforcement of data protection rules

In 2010, 96 perpetrators of unsolicited commercial communication were fined CZK 378,000 in total, and 106 inspections regarding compliance with the data protection rules ended up with sanctions of nearly CZK 5 million in total. Common breaches of data protection rules include wrongful information provided to the data subject and unsatisfactory security measures.

10.4 Judicial remedies

Since 2001, there have been 81 court proceedings dealing with decisions from the Office, with a 7:6 ratio in favour of the Office in 2010. In addition to this judicial review of administrative decisions, data subjects are entitled to seek judicial remedy via civil law actions, ie, should the breach of privacy cause any damage, or otherwise hampered personal rights, these are enforceable by a court. However, there were only few such cases decided by Czech courts – one was dealing with cameras in a block of flats (finding them inappropriate) and the others concerned mostly intrusions of journalists into celebrities' and politicians' privacy.

10.5 Class actions

Class actions are not permitted under Czech law.

10.6 Liability

The data controller shall be held liable for any damage caused as a result of an action in violation of the provisions of the Act. Data subjects that have incurred damage from an action in violation of the Act may thus claim damages from the data controller on the basis of civil liability for damages (as provided for in the Civil Code).

Privacy is not usually the object of court proceedings in the Czech Republic. However, two important cases have influenced the perception of privacy by the public.

The first (unpublished) case by a regional court concerned the monitoring by an employer of what the employee was viewing on the internet during working hours (as evidence that the employee was not working). Since the

case has not yet been dealt with by higher courts, clear guidance on the employer's and employee's rights regarding the monitoring of employees is still awaited.

The second case, Pl. ÚS 24/10, had legislative consequences – the Constitutional Court declared parts of the Act on Electronic Communications concerning traffic data retention unconstitutional. According to the Constitutional Court, the purposes for which the stored traffic and localisation data had to be provided to law enforcement authorities were not clearly and accurately defined, and therefore an assessment as to the actual necessity of such legal provisions could not be made. Until now, data retention in telecommunications has not been regulated and the government is preparing new legislation.

Denmark

DELACOUR DANIA Johnny Petersen

1. LEGISLATION

1.1 Name/title of the law

Act No. 429 of 31 May 2000 on Processing of Personal Data, as subsequently modified (*Lov om behandling af personoplysninger* (PDL)) provides the general legal framework for data protection in Denmark, which has implemented the Data Protection Directive 95/46/EC (the Directive).

According to section 2(1) of the PDL any rules on the processing of personal data contained in other legislation which give data subjects better legal protection shall take precedence over the rules laid down in the PDL. Such other rules may *inter alia* be found in the following legislation:

- Act on use of health information in the labour market;
- Act on securities trading;
- Act on financial business;
- Act on certain means of payment; and
- Act on tax control.

1.2 Pending legislation

A draft Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-user Terminal Equipment was presented by the National IT and Telecom Agency in May 2011 in order to implement Directive 2009/136/EC amending the ePrivacy Directive 2002/58/EC. No specific date has been fixed with regard to the Executive Order coming into force.

Although the deadline for the implementation of the Directive 2009/136/EC expired on 25 May 2011, Denmark has not yet implemented it.

1.3 Scope of the law

1.3.1 The main players

The 'data controller' is any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means for the processing of personal data.

The 'data processor' is any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller.

The 'personal data' are any information relating to an identified or identifiable natural person (the data subject).

The 'third party' is any natural or legal person other than:

(i) the data subject;
(ii) the data controller;

(iii) the data processor; and
(iv) anyone who, under the direct authority of the data controller or the data processor, is authorised to process the data.

1.3.2 Types of data

The PDL only covers personal data relating to natural persons and not data relating to legal persons (eg companies).

The PDL shall, however, apply to the processing of data concerning companies, etc, if the processing is *inter alia* carried out for credit information agencies or if the processing of data is carried out for the purpose of warning third parties against entering into business relations with a specific data subject.

'Personal data' are defined as '*any information relating to an identified or identifiable natural person, ie, the data subject*' and include an individual's name, photograph, telephone number, bank account number, etc.

The PDL basically distinguishes between three categories of personal data:

- ordinary personal data;
- sensitive data, ie, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership as well as the processing of data concerning health and sex life; and
- semi-sensitive data, ie personal data relating to criminal offences, severe social problems and other truly private matters falling outside the scope of sensitive data.

Personal data that have been made anonymous by removing any link to the identifiable person cannot be considered as personal data, provided the depersonalisation is absolute and cannot be reversed by any reasonable means likely to be used.

If data can be linked to an identified or identifiable person by means of a code, the data will continue to be considered as personal data.

1.3.3 Types of acts/operations

The PDL covers, as a general rule, the processing of personal data, defined as any operation or set of operations which is performed upon personal data, wholly or partly by automatic means, as well as otherwise than by automatic means if the personal data processed are included or are intended to be included in a filing system.

A filing system is defined 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.

1.3.4 Exceptions

The processing of personal data by a natural person in the course of purely personal or household activities falls outside the scope of the PDL.

Furthermore, the PDL shall not apply in the following circumstances:

- to the processing of data which is performed on behalf of the Danish Parliament (*Folketinget*) and its related institutions;
- to the processing of data covered by the Act on Information Databases

operated by the mass media;
- to information databases which exclusively include already published periodicals or sound and image programmes covered by paragraphs 1 or 2 of section 1 of the Act on Media Responsibility, provided that the data are stored in the database in the original version published. However, the rules regarding security measures and damages shall apply;
- to information databases which exclusively include already published texts, images and sound programmes which are covered by paragraph 3 of section 1 of the Act on Media Responsibility, provided that the data are stored in the database in the original version published. However, the rules regarding security measures and damages shall apply.
- to manual files of cuttings from published, printed articles which are exclusively processed for journalistic purposes. However, the rules regarding security measures and damages shall apply;
- to processing of data which otherwise take place exclusively for journalistic purposes shall be governed solely by the rules regarding security measures and damages. The same shall apply to the processing of data for the sole purpose of artistic or literary expression;
- to the processing of data which is performed on behalf of the intelligence services of the police and the national defence.

1.3.5 Geographical scope of application

The following two categories of data processing operations fall within the geographical scope of application of the PDL:
- The processing of personal data carried out on behalf of a data controller established in Denmark or in a place where Danish law applies by virtue of international public law if the activities are carried out within the territory of the European Union.
- The processing of personal data by a data controller with no permanent establishment in the EU, if the means used for the processing, which can be automatic or other means, are located on Danish territory, unless such equipment is used only for the purpose of transmitting data through the territory of the European Union; or the collection of personal data in Denmark takes place with a view to processing in a third country.

2. DATA PROTECTION AUTHORITY

Datatilsynet (The Danish Data Protection Agency)
Borgergade 28, 5.
1330 Copenhagen
DENMARK
T: +45 3319 3200
F: +45 3319 3218
E: dk@datatilsynet.dk
W: *www.datatilsynet.dk*

2.1 Role and tasks

The Data Protection Agency (*Datatilsynet*), which consists of a Council and a Secretariat, is responsible for the supervision of all processing operations covered by the PDL.

The day-to-day business is attended to by the Secretariat, headed by a Director. The Council, which shall be set up by the Minister of Justice, is composed of a chairman, who must be a legally qualified judge, and of six other members. Substitutes may be appointed for the members of the Council. The members and their substitutes shall be appointed for a term of four years. The Council shall lay down its own rules of procedure and detailed rules on the division of work between the Council and the Secretariat.

The Data Protection Agency must act with complete independence in executing the functions entrusted to it. The Data Protection Agency must supervise, on its own initiative or acting on a complaint from a data subject, that the processing of personal data is carried out in compliance with the provisions of the PDL and any rules issued by virtue of this Act.

No administrative appeals may be brought before any other administrative authority against the decisions made by the Data Protection Agency under the provisions of the PDL; however, the decisions of the Data Protection Agency may be challenged in court.

The Data Protection Agency may ask to be furnished with any information of importance to its activities, including for the decision as to whether or not a particular matter falls under the provisions of the PDL.

2.2 Powers

The members and the staff of the Data Protection Agency shall, at any time, against appropriate proof of identity and without any court order, have access to all premises from which processing operations carried out on behalf of the public administration are administered, or from which there is access to the data subject to processing, and to all premises where data or technical equipment are stored or used.

For the enforcement powers of the Data Protection Agency, see section 10.1 below.

The Data Protection Agency may decide that notifications and applications for authorisations under the provisions of the PDL and any changes may or shall be submitted in a specified manner.

The Data Protection Agency must submit an annual report on its activities to the Danish Parliament (*Folketinget*), which shall be made public. The Data Protection Agency may also make its opinions accessible to the general public.

2.3 Priorities

The Data Protection Agency's priorities in 2010 were *inter alia*:

- supervision of companies' implementation of whistleblowing schemes; and
- supervision of social networks, such as Facebook.

Apparently, these priorities have also been pursued in 2011.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Consent constitutes one of the possible legal bases for the rightful processing of non-sensitive personal data, semi-sensitive data as well as sensitive data.

The data subject's consent is defined as '*any freely given, specific and informed indication of her/his wishes by which the data subject signifies her/his agreement to the processing of personal data relating to the data subject*'.

'Specific' means that the consent must be concrete to the effect that it clearly and unambiguously states what the consent covers. 'Informed' means that the data subject must be fully aware of what the consent covers.

3.1.2 Form

In principle, the PDL does not require consent to be given in a specific form.

As the burden of proof with regard to having obtained consent lies with the data controller it is, however, always recommended to obtain written consent in order to ensure clarity with regard to the scope of the consent.

3.1.3 In an employment relationship

There are no barriers with regard to an employee giving consent to the employer's processing of personal data regarding the employee.

3.2 Other legal grounds for data processing

Non-sensitive personal data may be processed if one or more of the following conditions are met:

- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary for the performance of a task carried out in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed; and
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

Semi-sensitive personal data may be processed by private companies and bodies without the data subject's explicit consent if one or more of the following conditions are met:

- the data are processed for the purpose of pursuing public or private interests, including the interests of the person concerned, which clearly override the data subject's interests of secrecy; and

- if any of the conditions laid down in section 7 of the PDL (regarding sensitive data) are satisfied.

Sensitive data may be processed by private companies and bodies without the data subject's explicit consent if one or more of the following conditions are met:

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

Furthermore, processing of data concerning trade union membership may further take place where the processing is necessary for the data controller's compliance with labour law obligations or specific rights.

Processing may also take place where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where those data are processed by a health professional subject under law to the obligation of professional secrecy.

Furthermore, processing of data may take place where the processing is required for the performance by a public authority of its tasks in the area of criminal law.

3.3 Direct marketing and cookies

The processing of personal data for the purpose of direct marketing is subject to the general provisions of the PDL. In addition, the PDL contains specific provisions on direct marketing.

A company may not disclose data concerning a consumer to a third company for the purpose of marketing or use such data on behalf of a third company for this purpose, unless the consumer has given his explicit consent. The consent shall be obtained in accordance with the rules laid down in section 6 of the Danish Marketing Practices Act.

However, the disclosure and use of such data may take place without consent: (i) in the case of general data on customers which form the basis for classification into customer categories; and (ii) provided processing is necessary for the purpose of the legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, and provided these interests are not overridden by the interests of the data subject. The latter shall normally be the case.

Furthermore, if a consumer objects, a company may not disclose data relating to that person to a third company for the purposes of marketing or use the data on behalf of a third company for such purposes.

Before a company discloses data concerning a consumer to a third company for the purposes of marketing or uses the data on behalf of a third company for such purposes, it must always check in the CPR-register (the national Danish database including a unique identification number

for all Danish inhabitants) whether the consumer has filed a statement to the effect that she/he does not want to be contacted for the purpose of marketing activities. Before data relating to a consumer who has not given such information to the CPR-register are disclosed or used as mentioned, the company shall provide information about the right to object to the disclosure/use of the data in a clear and intelligible manner. At the same time, the consumer shall be given access to object in a simple manner within a period of two weeks. The data may not be disclosed until the time limit for objecting has expired.

Contact with consumers must always take place in accordance with the rules laid down in section 6 of the Danish Marketing Practices Act.

The use of cookies or equivalent devices is regulated in Article 5(3) of Directive 2002/58/EC on the protection of privacy in the electronic communications sector (the ePrivacy Directive), as amended by Directive 2009/136/EC, which amends in particular Article 5(3) of the ePrivacy Directive and contains stricter rules on the use of cookies. Although the deadline for the implementation of the Directive expired on 25 May 2011, Denmark has not yet implemented it. Presently, Danish law stipulates an opt-out approach with regard to use of cookies.

3.4 Data quality requirements

Data controllers must ensure lawful processing of personal data in accordance with good standards for processing of personal data.

Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

Moreover, only personal data that are relevant and not excessive in relation to the purposes for which they are collected and/or further processed, are kept up-to-date and kept in a form permitting identification of data subjects for no longer than necessary may be processed.

3.5 Outsourcing

When outsourcing data processing activities to data processors, the data controller is required to:

(i) select a data processor which will take the necessary security measures;
(ii) supervise the data processor's compliance with these security measures; and
(iii) enter into a written agreement with the data processor. The written agreement must:
    - specify the technical and organisational security measures; and
    - stipulate that the data processor will only act on behalf of the data controller.

If the data processor intends to sub-contract the data processing, and this is not explicitly permitted by the contract, the processor must inform the data controller of this intention. In addition, the processor must ensure that the same obligations that apply to the data processor under the controller-processor agreement also apply to the sub-processor.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use as well as the use of surveillance cameras are subject to the provisions of the PDL. Specific rules on use of surveillance cameras are contained in Chapter 6a of the PDL (sections 26a-26c).

Moreover, the Danish Criminal Code and the Act on Video Surveillance (Consolidated Act No. 788 of 12 August 2005 with later amendments) contain specific provisions on the installation and use of surveillance cameras.

Section 26a PDL regulates the transfer and deletion of image and sound recordings including personal data collected in relation to the prevention of crime. Other questions regarding transfer and deletion are regulated by the general rules of the PDL.

PDL section 26a does, however, not deal with the question as to what extent video surveillance making use of image and sound recordings may rightfully take place. Rather, the private entities' right to conduct video surveillance making use of image and sound recordings is regulated by the Act on Video Surveillance with regard to places with ordinary access and by the Criminal Code with regard to places with no ordinary access.

According to the Act on Video Surveillance, the basic rule is that private entities may not conduct video surveillance of *inter alia* streets, squares and any other places used for ordinary traffic.

However, private entities may, under certain conditions, conduct video surveillance in the following situations:

video surveillance may be conducted by the owner of gas stations, factory premises, covered shopping areas and corresponding areas;

- video surveillance may be conducted by the owner of cash dispensers, foreign exchange machines and money transportation vehicles;
- video surveillance is permitted of entrances and fronts of banks, casinos, hotels, restaurants, shopping centres and stores from which retail sales take place; and
- video surveillance is permitted by the owner of entrances, fronts, enclosures and corresponding areas, provided that no recordings of the surveillance are made.

3.6.2 Employment relationship

The Danish Data Protection Agency has considered in a number of cases the legal guidelines for the control by a public or private employer over employees' use of the internet and email correspondence.

In summary, the state of the law may be described as follows. A public authority as well as a private company may, based on management, operational and security considerations, decide whether or not to issue guidelines regarding the control over the use of that authority's or company's IT-systems.

It is, however, a legal requirement that the employees are clearly and explicitly informed beforehand of the fact that such control shall take place.

In relation to the control of email correspondence, it is a requirement that

the company may not read email correspondence identified as 'private'. This requirement follows from the Danish Criminal Code.

The Data Protection Agency encourages companies to include the issue of employees' use of the internet and email correspondence in relation to the company's IT-system in discussions in the company's works committee or similar bodies.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers are responsible for informing the data subjects about the processing of personal data relating to them.

4.2 What

Unless the data subject is already aware of this, the data controller must provide the following information to the data subject:

- the name and address of the data controller and of her/his representative, if any; and
- the purpose(s) of the data processing.

Depending on the situation at hand, it may be necessary to provide additional information to guarantee the fair processing of the data. Such information may include:

- the recipients of the data;
- whether a reply to the request for personal data is obligatory or voluntary, as well as the possible consequences of a failure to reply; and
- the existence of the right of access to, and the right to rectify, the personal data concerning the data subject.

4.3 Exceptions

The data controller is exempt from providing the above information if:

- the data subject is already aware of the information;
- providing this information proves impossible or would require a disproportionate effort; or
- recording or disclosure of the data is expressly laid down by law or in accordance with law.

The data controller's information obligation shall not apply if the data subject's interest in obtaining this information is found to be overridden by essential private interest considerations, including considerations about the data subject herself/himself.

Derogations from the data controller's information obligation may also take place if the data subject's interest in obtaining this information is found to be overridden by essential considerations of public interest, including in particular:

- national security;
- defence;
- public security;
- the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions;

- important economic or financial interests of a member state or of the European Union, including monetary, budgetary and taxation matters; and
- monitoring, inspection or regulatory functions, including temporary tasks, connected with the exercise of official authority in cases referred to in points (iii) to (v).

4.4 When

The information should be provided at the time the personal data are recorded. When the data are not obtained directly from the data subject, the information should be provided at the time the personal data are recorded, or when a disclosure to a third party is envisaged, but no later than the first time the data are disclosed.

4.5 How

The PDL does not specify in which form and how the information must be provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access to data

5.1.1 Right

When a person submits a request to that effect, the data controller shall inform her/him whether or not data relating to her/him are being processed. Where such data are being processed, communication with her/him shall take place in an intelligible form about:

- the data that are being processed;
- the purposes of the processing;
- the categories of recipients of the data; and
- any available information as to the source of such data.

No specific formalities apply with regard to the request for access to data. A request for access to data may thus be made orally, by post or by email.

5.1.2 Exceptions

The data controller is exempt from providing the requested information if:

- the data subject is already aware of the information;
- providing this information proves impossible or would require a disproportionate effort; or
- recording or disclosure of the data is expressly laid down by law or in accordance with law.

The data controller's obligation to provide access to data shall not apply if the data subject's interest in obtaining this information is found to be overridden by essential private interest considerations, including considerations about the data subject herself/himself.

Derogations from the data controller's obligation to provide the requested information may also take place if the data subject's interest in obtaining this information is found to be overridden by essential public interest considerations, including in particular:

- national security;
- defence;
- public security;
- the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions;
- important economic or financial interests of a member state or of the European Union, including monetary, budgetary and taxation matters; and
- monitoring, inspection or regulatory functions, including temporary tasks, connected with the exercise of official authority in cases referred to in points (iii) to (v).

Further exemptions follow from section 32(2)-32(5) of the PDL.

5.1.3 Deadline

The data subject can exercise the right to access at any time. In response, the data controller must communicate the information without delay, and at the very latest within four weeks after receipt of the request. If the request has not been replied to within four weeks from the receipt of the request, the data controller shall inform the person in question of the reasons for this and of the time at which the decision can be expected to be available.

A data subject who has received a reply to a request for access to data shall not be entitled to a new reply to a request for access to data until six months after the last communication, unless she/he can establish that she/he has a specific interest to that effect.

A response to a request for access to data shall be made in writing, if requested. In cases where it is favourable to the interests of the data subject, the communication may, however, be given orally about the contents of the data.

5.1.4 Charges

The Minister of Justice may lay down rules regarding the payment for written responses by private companies to data subject's requests. Such rules have been stipulated in Statutory Order No. 533 of 15 June 2000 regarding private data controllers' written responses to requests for access to data. According to these rules private data controllers may request data subjects to pay DKK 10 per page provided. The total payment may, however, not exceed DKK 200.

5.2 Rectification

5.2.1 Right

The data controller shall at the request of the data subject rectify personal data which turn out to be inaccurate or misleading or are in any other way processed in violation of law or regulations.

The data controller shall, at the request of the data subject, notify third parties to whom the data have been disclosed of any rectification carried out. However, this shall not apply if such notification proves impossible or involves a disproportionate effort.

5.2.2 Exceptions
There are no exceptions to the right to rectification.

5.2.3 Deadline
The data controller must rectify the personal data as soon as reasonably possible after the submission of the data subject's request.

5.2.4 Charges
The data subject shall not be charged for exercising the right to rectification.

5.3 Erasure
5.3.1 Right
The data controller shall, at the request of the data subject, erase data which turn out to be inaccurate or misleading or are in any other way processed in violation of law or regulations.

The data controller shall, at the request of the data subject, notify any third parties to whom the data have been disclosed of any erasure carried out. However, this shall not apply if such notification proves impossible or involves a disproportionate effort.

5.3.2 Exceptions
There are no exceptions to the right to erasure.

5.3.3 Deadline
The data controller must erase the personal data as soon as reasonably possible after the submission of the data subject's request.

5.3.4 Charges
The data subject shall not be charged for exercising the right to erasure.

5.4 Blocking
5.4.1 Right
The data controller shall, at the request of the data subject, block data which turn out to be inaccurate or misleading or are in any other way processed in violation of law or regulations.

The data controller shall, at the request of the data subject, notify any third parties to whom the data have been disclosed of any blocking carried out. However, this shall not apply if such notification proves impossible or involves a disproportionate effort.

5.4.2 Exceptions
There are no exceptions to the blocking right.

5.4.3 Deadline
The data controller must block the personal data as soon as reasonably possible after the submission of the data subject's request.

5.4.4 Charges
The data subject shall not be charged for exercising the blocking right.

5.5 Objection
5.5.1 Right
A data subject may at any time object to the data controller in relation to the processing of personal data relating to him.

Where an objection is justified, the processing may no longer involve those data.

5.5.2 Exceptions
There are no exceptions to the objection right.

5.5.3 Deadline
The data controller must, based on a justified objection, end all processing of the relevant personal data as soon as reasonably possible after the submission of the data subject's request.

5.5.4 Charges
The data subject shall not be charged for exercising the right to object.

5.6 Automated individual decisions
5.6.1 Right
Where the data subject objects, the data controller may not make her/him subject to a decision which produces legal effects concerning or significantly affecting her/him and which is based solely on automated processing of data intended to evaluate certain personal aspects.

5.6.2 Exceptions
The right shall not apply if that decision:

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard her/his legitimate interests; or
- is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

5.6.3 Deadline
The data subject has a right to be informed by the data controller as soon as possible and without undue delay about the rules on which an automated decision is based.

5.6.4 Charges
The data subject shall not be charged for exercising his right.

5.7 Other rights
A data subject may always withdraw consent given to the processing of

personal data.

A data subject may at all times file a complaint to the appropriate supervisory authority (eg, the Data Protection Agency) concerning the processing of data relating to her/him.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

Prior to the commencement of any processing of personal data which is carried out on behalf of a private data controller, the controller or his representative must notify the Danish Data Protection Agency. In practice, a number of exceptions apply to this main rule.

6.1.2 What

The notification must include the following information:

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

6.1.3 Exceptions

Processing of personal data shall, as a starting point, be exempt from the notification obligation under the following circumstances:

- the processing relates to data about employees, to the extent that the processing does not include sensitive or semi-sensitive data;
- the processing relates to data concerning the health of employees, to the extent that the processing of health data is necessary to comply with provisions laid down by law or regulations;
- the processing relates to data concerning employees if registration is necessary under collective agreements or other agreements in the labour field;
- the processing relates to data concerning customers, suppliers or other business relations, to the extent that the processing does not include sensitive or semi-sensitive data;
- the processing is carried out for the purpose of market surveys, to the extent that the processing does not include sensitive or semi-sensitive data;
- the processing is carried out by an association or similar body, to the

extent that only data concerning the members of the association are processed;
- the processing is carried out by lawyers or accountants in the course of business, to the extent that only data concerning client matters are processed;
- the processing is carried out by doctors, nurses, dentists, dental technicians, chemists, therapists, chiropractors and other persons authorised to exercise professional activities in the health sector, to the extent that the data are used solely for these activities and the processing of the data is not carried out on behalf of a private hospital; or
- the processing is carried out for the purpose of being used by an occupational health service.

The Minister of Justice may lay down rules to the effect that other types of processing operations shall be exempt from the notification obligation. Such rules have been laid down in Statutory Order No. 534 of 15 June 2000. By this statutory order *all* processing of personal data shall as a starting point be exempted from the notification obligation, unless one of the following circumstances are applicable:
- the processing includes sensitive or semi-sensitive data;
- the processing of data is carried out for the purpose of warning third parties against entering into business relations or an employment relationship with a data subject;
- the processing is carried out for the purpose of disclosure, in the course of business, of data for assessment of financial standing and creditworthiness;
- the processing is carried out for the purpose of professional assistance in connection with staff recruitment; or
- the processing is carried out solely for the purpose of operating legal information systems.

6.1.4 When
Notification must be made prior to starting any processing activity.

6.1.5 How
Notification may be made online on the Data Protection Agency's website (*www.datatilsynet.dk*) or by completing a hard copy notification form and sending it to the Data Protection Agency. Standard notification forms and guidelines are available on the Data Protection Agency's website.

Guidance with respect to the notification procedure is available in Guidelines No. 125 of 10 July 2000 regarding notification in accordance with Chapter 12 of the PDL.

In 2010, the Data Protection Agency received a total of 2,660 notifications.

6.1.6 Notification fees
An amount of DKK 1,000 shall be payable in connection with the submission of the following notifications and applications for authorisation under the PDL:

- notifications;
- authorisations; and
- notifications of providers offering electronic processing services.

Such notifications and authorisations shall be deemed to have been submitted only when payment of the stipulated fee has been made.

Where a processing operation shall both be notified under PDL and authorised under PDL only a single fee shall be payable.

6.2 Authorisation requirements

In principle, data controllers do not need to obtain authorisation to carry out data processing activities. However, prior to the commencement of any data processing which is subject to the obligation to notify, the authorisation of the Data Protection Agency must be obtained in the following circumstances:

- the processing includes sensitive or semi-sensitive data;
- the processing of data is carried out for the purpose of warning third parties against entering into business relations or an employment relationship with a data subject;
- the processing is carried out for the purpose of disclosure, in the course of business, of data for assessment of financial standing and creditworthiness;
- the processing is carried out for the purpose of professional assistance in connection with staff recruitment; or
- the processing is carried out solely for the purpose of operating legal information systems.

Furthermore, in the case of international transfers of personal data to third countries the authorisation of the Data Protection Agency for such transfer must be obtained, regardless of the processing being otherwise exempt from the obligation to notify, if the transfer of personal data is made based on one of the following conditions:

- the personal data are transferred to a third country that ensures an adequate level of protection;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

The Data Protection Agency may, when granting an authorisation, lay down specific conditions for the carrying out of the processing operations for reasons of the protection of the privacy of the data subjects.

Authorisations may be requested online on the Data Protection Agency's website (*www.datatilsynet.dk*) or by completing a hard copy notification form and sending it to the Data Protection Agency. Standard forms and guidelines are available on the Data Protection Agency's website.

6.3 Register

The Data Protection Agency maintains a public register of notified processing operations which may be consulted by anyone, free of charge, at *www.datatilsynet.dk*. For each processing, the public register contains the same information as is provided in the notification form.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Under the PDL it is not mandatory to appoint a data protection officer, and in practice companies (data controllers) do not appoint a data protection officer.

7.2 Tasks and powers

Not applicable.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

In principle, personal data may only be transferred to a third country if that country ensures an adequate level of protection.

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation, in particular the nature of the data; the purpose and duration of the processing operation; the country of origin and country of final destination of the personal data; the rules of law in force in the third country in question; and the professional rules and security measures which are complied with in that country. The European Commission has recognised several countries to provide an adequate level of protection.

Data transfers from Denmark to other EEA member states are not subject to the rules on international data transfers, as EEA member states are not considered to be 'third countries'.

Data transfers to countries outside the EEA that have not been recognised as providing an adequate level of protection (that is, unsafe third countries) are in principle prohibited, subject to exceptions.

8.2 Legal basis for international data transfers

Data may be transferred to unsafe third countries if one or more of the following criteria are met:

- the data subject has given her/his explicit consent;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data

subject;
- the transfer is made from a register which according to law or regulations is open to consultation either by the public in general or by any person who can demonstrate legitimate interests, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;
- the transfer is necessary for the prevention, investigation and prosecution of criminal offences, the execution of sentences or the protection of persons charged, witnesses or other persons in criminal proceedings; or
- the transfer is necessary to safeguard public security, the defence of the realm, or national security.

8.2.1 Data transfer agreements

Authorisation for the transfer of personal data to an unsafe third country may be obtained from the Data Protection Agency if the data controller provides sufficient guarantees in the form of data transfer agreements that are, for instance, based on one of the European Commission's standard contractual clauses for data transfers to third countries.

8.2.2 Binding corporate rules

If a data transfer is based on binding corporate rules, such data transfer must be authorised by the Data Protection Agency. Denmark takes part in the mutual recognition procedure.

The authorisation request may be based on the Article 29 Working Party's Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (WP133).

8.2.3 Safe Harbour

Personal data may also be transferred to organisations in the US that are certified under the US 'safe harbour' scheme provided that the data transfer falls into the scope of that certification. In such case there is no need to obtain the data subject's consent or to rely on one of the other exceptions listed in section 8.2 above.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The PDL requires data controllers and data processors to ensure the confidentiality and security of personal data. In particular, confidentiality is regarded as an organisational security measure.

9.2 Security requirements

Individuals, companies etc performing work for the data controller or the data processor and who have access to personal data may process them only on instructions from the data controller unless otherwise provided by law or regulations.

Such instructions may, however, not restrict journalistic freedom or

impede the production of an artistic or literary product.

The data controller shall implement appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down in the PDL. The same shall apply to data processors.

The Minister of Justice may lay down more detailed rules concerning such security measures. Based on this authorisation, the Minister of Justice has issued Statutory Order No. 528/2000 on security measures for protection of personal data processed by public authorities. Private data controllers may, however, look to the provisions of this statutory order when seeking guidance with regard to specific security measures.

Where a data controller leaves the processing of personal data to a data processor, the data controller shall make sure that the processor is in a position to implement the required technical and organisational security measures and must ensure compliance with those measures.

The carrying out of processing by way of a data processor must be governed by a written contract between the parties. This contract must stipulate: (i) that the data processor shall act only on instructions from the data controller; and (ii) that the rules concerning appropriate technical and organisational security measures shall also apply to processing by way of a data processor. If the data processor is established in a different member state, the contract must stipulate that the provisions on security measures laid down by the law in the member state in which the data processor is established are fulfilled.

9.3 Data security breach notification obligation

There is no obligation under Danish law to notify personal data security breaches to the data subjects and/or to the Data Protection Agency.

9.4 Data protection impact assessments and audits

There is no general requirement to carry out data protection impact assessments and audits as such under Danish law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement actions

The Data Protection Agency may carry out targeted inspections on its own initiative. In addition, the Data Protection Agency may investigate any complaints it receives.

The Data Protection Agency may order a private data controller to discontinue a processing operation which may not take place under the PDL and to rectify, erase or block specific data undergoing such processing.

The Data Protection Agency may also prohibit a private data controller from using a specific procedure in connection with the processing of data if the Data Protection Agency finds that the procedure in question involves a considerable risk to the effect that the data are processed in violation of the PDL.

Furthermore, the Data Protection Agency may order a private data controller to implement specific technical and organisational security measures to protect data which may not be processed against processing, and to protect data against accidental or unlawful destruction or accidental loss, alteration, and disclosure to any unauthorised person, abuse or any other unlawful forms of processing.

Finally, the Data Protection Agency may in special circumstances issue a prohibitory or mandatory injunction against data processors.

The Data Protection Agency may carry out on-site investigations. In the course of the investigation, the data controller must provide all necessary information upon request and co-operate with the Data Protection Agency.

According to the Data Protection Agency's latest annual report (2010) it initiated 65 audits of individual data controllers in 2010.

10.2 Sanctions

In the absence of more severe sanctions being prescribed under other legislation, any person who commits any of the following offences in connection with the processing of personal data carried out on behalf of private individuals or bodies shall be liable to a fine or imprisonment of up to four months:

- violation of certain of PDL's provisions regarding processing of personal data; transfer of personal data to third countries; data subjects rights; security measures; and notification/authorisation obligations;
- failure to comply with the Data Protection Agency's decisions in accordance with certain of the provisions of the PDL.;
- failure to comply with the Data Protection Agency's requests for information;
- obstruction of the Data Protection Agency's requests for access to premises;
- failure to comply with specific conditions in relation to processing of personal data; transfer of data to third countries; or any terms or conditions stipulated for authorisation in accordance with rules issued by virtue of the PDL;
- failure to comply with prohibitory or mandatory orders or in accordance with rules issued by virtue of the PDL.

In the absence of more severe sanctions being prescribed under other legislation, any person who in connection with a processing operation carried out on behalf of public authorities violates rules on security measures or approval as IT service provider, or fails to comply with certain conditions as referred to in PDL regarding processing of personal data and transfer of data to third countries or any terms or conditions for authorisation in accordance with rules issued by virtue of PDL, shall be liable to a fine or imprisonment of up to four months.

In the absence of more severe punishment being prescribed under other legislation, any person who in connection with a processing operation governed by another member state's legislation fails to comply with the decisions of the Data Protection Agency or to fulfil the requirements of the

Data Protection Agency with regard to providing information or obstructs the Data Protection Agency's right of access, shall be liable to a fine or imprisonment of up to four months.

Criminal liability may be imposed on companies, etc (legal persons) pursuant to the rules laid down in the Danish Criminal Code.

The level of fines imposed on companies due to violations of the PDL typically falls within the range of DKK 5,000-DKK 25,000.

10.3 Examples of recent enforcement of data protection rules

In practice the most important tool with regard to enforcing the PDL is the Data Protection Agency's competence to carry out targeted inspections on its own initiative or based on complaints from data subjects and third parties. The Data Protection Agency regularly makes use of this competence.

A recent, significant example of the Data Protection Agency's enforcement of the PDL took place in August 2011, when the left-wing organisation REDOX publicised on the internet an extensive report with substantial information on a large number of individuals who were allegedly members of various right-wing political organisations. The Data Protection Agency was of the opinion that the PDL had been seriously violated by the publication of personal data regarding individuals' political opinion, and the matter was turned over to the police by the Data Protection Agency. The police investigation, according to the available information, is still pending.

10.4 Judicial remedies

The courts may become involved in the enforcement of the PDL in two different ways.

Firstly, in relation to a civil action whereby a data subject is claiming damages (injury to a person's reputation) with reference to a data controller having acted contrary to the PDL. Secondly, in relation to a criminal action which is initiated by the prosecution after it has been referred to it by the Data Protection Agency.

A few cases regarding civil action have been tried by the courts. For instance, in a case decided by the Maritime and Commercial Court on 6 December 2007 a former employee was awarded DKK 25,000 in damages with reference to illegal video surveillance by the employer contrary to the PDL.

The sanctions imposed in such cases have generally been fines within the range of DKK 5,000 to 25,000.

10.5 Class actions

Class actions are permitted, but rarely used under Danish law, and there are no examples of class actions based on violations of the PDL.

10.6 Liability

The data controller may be liable for damages (injury to a person's reputation) due to breach of the PDL, 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, and a person suffering harm as a

consequence of acts infringing the provisions of the PDL can initiate a civil action for damages.

European Union

Van Bael & Bellis Monika Kuschewsky

1. LEGISLATION

1.1 Name/title of the law

In the EU, the collection and processing of personal data is regulated by 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 (the Directive).

The EU data protection legal framework is based on the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which was the first binding international legal instrument for data protection. All EU member states are bound by this Convention.

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive) contains more specific rules concerning the processing of personal data in the electronic communications sector. The ePrivacy Directive was amended in 2009 by Directive 2009/136/EC of 25 November 2009. Most of the new obligations only apply to providers of publicly available electronic communications services, such as the new data security breach notification obligation. However, the amendments also contain some new general obligations, eg, stricter rules on the use of cookies (see also section 3.3 below). The deadline for the implementation of this Directive expired on 25 May 2011.

Activities falling under the former 'second' and 'third pillar' of the EU are excluded from the scope of application of the Directive. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, for instance, regulates the processing of personal data in the former 'third pillar' of the EU.

The Lisbon Treaty, which entered into force on 1 December 2009, has abolished the 'pillar structure' and has introduced Article 16 of the Treaty on the Functioning of the EU to the EU data protection legal framework. Article 16, which confers on all individuals the right to the protection of their personal data, has general application and also applies to the area of law enforcement.

Moreover, the right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights, which was given binding legal effect by the Lisbon Treaty.

1.2 Pending legislation

The Directive is currently under review and the European Commission is expected to present a legislative proposal not before the end of 2011. It is still unclear if the new legal instrument will take the form of a directive or a regulation.

The European Commission's strategy for the reform, as set out in its Communication of 4 November 2010, contains five key objectives:

(1) strengthening individuals' rights, eg, by strengthening the principle of data minimisation and improving the modalities for the exercise of individuals' rights (see also section 5 below);
(2) enhancing the internal market dimension, eg, by simplifying and harmonising registration formalities in EU member states (see also section 6 below);
(3) ensuring a high level of protection for international data transfers, eg, by streamlining, clarifying and simplifying the current procedures for international data transfers, including with respect to the Commission's standard contractual clauses and binding corporate rules (see also section 8 below);
(4) a more effective enforcement of the data protection rules, eg, by extending the power to bring an action before courts both to national data protection authorities and to other associations representing data subjects' interests (see also section 10 below); and
(5) revising the data protection rules in the area of police and judicial cooperation in criminal matters, eg, by considering the extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters.

In parallel, the Council of Europe is reviewing Convention 108 and is also expected to present proposals for amending the Convention by the end of 2011.

1.3 Scope of the law

1.3.1 The main players

- The 'data controller' is any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
- The 'data processor' is any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
- The Article 29 Working Party (the Working Party), which is an independent EU advisory body on data protection and privacy, set up under Article 29 of the Directive (see also section 2 below), has clarified the definitions of 'data controller' and 'data processor' in its Opinion WP 169.
- The 'data subject' is any identified or identifiable natural person which can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.
- The 'third party' is any natural or legal person, public authority, agency

or any other body other than the data subject, the data controller, the data processor and the persons who, under the direct authority of the data controller or the data processor, are authorised to process the personal data.

1.3.2 Types of data

'Personal data' are defined as 'any information relating to an identified or identifiable natural person (the data subject)'.

The Working Party has clarified in its Opinion WP 136 that 'personal data' include biometric data, IP addresses and pseudonymised data, but not anonymous data.

In addition, the Directive lists three special categories of personal data that are subject to stricter processing conditions: (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life ('sensitive data'); (ii) personal data relating to offences, criminal convictions or security measures ('judicial data'); and (iii) national identification numbers or any other identifiers of general application.

1.3.3 Types of acts/operations

The Directive covers both manual as well as automatic processing of personal data. The processing of personal data is defined as '*any operation or set of operations which is performed upon personal data, wholly or partly by automatic means*', eg, by means of a computer. The definition also includes processing otherwise than by automatic means of personal data which (are intended to) form part of a filing system. A 'filing system' is defined 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*'.

The Directive gives the following examples of data processing: the collection; recording; organisation; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission; dissemination or otherwise making available; alignment or combination; blocking; erasure; or destruction of personal data.

1.3.4 Exceptions

The Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of EU law and to processing operations concerning public security, defence, state security (including the economic well-being of the state when the processing operation relates to state security matters) and the activities of the state in areas of criminal law.

The Directive also does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

1.3.5 Geographical scope of application

As regards the applicable law, the Directive distinguishes between whether the data controller is established in the EU or not.

If the data controller is established in an EU member state and the processing is carried out in the context of the activities of that establishment, the national law of that EU member state, implementing the Directive, applies to the processing of personal data.

The notion of establishment is not defined in the Directive. The preamble of the Directive indicates however that '*establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; […] the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect*'.

If the data controller is not established in the EU, the national law of an EU member state implementing the Directive applies to the processing of personal data if:

- that EU member state's law applies by virtue of international public law (eg, on a ship or in an embassy); or
- the data controller, for purposes of processing personal data, makes use of equipment situated on that EU member state's territory. The Working Party understands the word 'equipment' as 'means' (eg, cars that collect Wi-Fi information while circulating on the streets). However, the national law will not apply if such equipment is used only for purposes of transit through the territory of the Community.

If the data controller makes use of equipment situated in an EU member state, he must designate a representative established in the territory of that member state.

The rules on the applicable law have been clarified by the Working Party in its Opinion WP 179.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Each of the EU member states has designated a supervisory authority (the national data protection authorities) responsible for monitoring the application within that EU member state of the Directive as implemented by that EU member state.

These authorities shall act with complete independence in exercising the functions entrusted to them (the notion of independence has been interpreted in a judgment rendered by the EU's Court of Justice in March 2010). Article 28 of the Directive contains further details regarding the supervisory authorities, including the powers with which they should be endowed.

On the EU level, there are three main players:

- the European Commission, which is the EU's executive body;
- the Working Party; and
- the European Data Protection Supervisor (the EDPS).

The national data protection authorities of each EU member state are represented in the Working Party, together with the EDPS and the European Commission.

The Working Party
Website: *http://ec.europa.eu/justice/data-protection/article-29/index_en.htm*

The EDPS
Rue Montoyer 63,
1000 Brussels, Belgium
T: +32 2 283 19 00
F: +32 2 283 19 50
E: edps@edps.europa.eu
W:*www.edps.europa.eu*

2.1 Role and tasks

The national data protection authorities monitor and enforce the national data protection laws in the respective EU member states. They also hold a public register of notified processing operations (see section 6.4 below).

The European Commission tables proposals for new data protection legislation, engages in dialogue with third countries and negotiates international agreements and adopts adequacy decisions (see section 8.1 below).

The Working Party's tasks are listed in Article 30 of the Directive and Article 15(3) of the ePrivacy Directive and include adopting non-binding opinions and recommendations.

The objectives of the Working Party are to:

- provide expert opinion to the European Commission on questions of data protection law;
- promote the uniform application of the EU data protection legal framework through co-operation between data protection authorities;
- advise the European Commission on any Community measures with regard to the processing of personal data and privacy; and
- make recommendations on matters relating to the processing of personal data and privacy.

The EDPS is an independent authority established by Regulation 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. He supervises the processing of personal data in the EU administration, advises on proposals for new legislation having an impact on data protection and cooperates with other data protection authorities in order to promote consistent data protection throughout Europe.

2.2 Powers

The powers of the national data protection authorities are laid down in the national data protection laws. They may have:

- investigative powers;
- powers of intervention, such as the power to exercise certain rights on behalf of the data subjects (see also section 5 below);
- the power to engage in legal proceedings or to bring violations of the national data protection laws to the attention of the judicial authorities;

- sanctioning powers;
- the power to issue decisions, eg, to authorise a data processing.

The European Commission has the power to open infringement proceedings against an EU member state which it considers to infringe the EU data protection legislation. The European Commission will try to bring the infringement to an end. If necessary, it may refer the case to the Court of Justice of the European Union.

2.3 Priorities

The Working Party publishes its work programmes on its website. According to the 2010-2011 Work Programme (WP 170), the Working Party intends to concentrate on:

- implementing the Directive and preparing a future comprehensive legal framework;
- addressing globalisation;
- responding to technological challenges; and
- making the Article 29 Working Party and data protection authorities more effective.

The European Commission's priorities for 2010-2011 are the reform of the Directive and the implementation of the amendments brought to the ePrivacy Directive in 2009.

According to the EDPS' Annual Report for 2010, the EDPS intends to monitor the ongoing review of the Data Retention Directive 2006/24/EC and monitor the implementation of new technologies as foreseen under the EU's Digital Agenda.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

Consent is one of the possible legal bases for the processing of personal data, but not judicial data.

3.1.1 Definition

The data subject's consent is defined as *'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'*

In its Opinion WP 187, the Working Party explains the notion of consent on the basis of a detailed analysis of the key elements of this definition:

- '*any …. indication of his wishes … signifying …*' means that consent requires active behaviour from the data subject.
- '*freely given*' means that the data subject must have a real choice. There should not be any risk of deception, intimidation, coercion or significant negative consequences. Nevertheless, a moderate incentive for the data subject to consent, such as a small reduction in a fee, is permitted.
- '*specific*' means that the consent must be intelligible, refer clearly and precisely to the scope and consequences of the data processing and must be given in relation to the different aspects of the processing, ie, which

personal data are processed and for which purposes. The Working Party recognises that it should be sufficient for controllers to obtain consent only once for different operations that fall within the reasonable expectations of the data subject.
- '*informed*' means that consent must be based on an appreciation and understanding of the facts and implications of an action. This implies that the data subject is given accurate and full information of all relevant issues, including those specified in Articles 10 and 11 of the Directive regarding the information obligations *vis-à-vis* the data subjects.

3.1.2 Form

Consent must be '*unambiguous*' to form a legal basis for the processing of normal categories of data as well as for data transfers to non-adequate third countries (see section 8.2 below).

In its Opinion WP 187, the Working Party explains that, for consent to be unambiguous, the procedure to seek and to give consent must leave no doubt as to the data subject's intention to deliver consent.

For the processing of sensitive data, consent must be '*explicit*'. Consent can be given in writing or orally, but for evidentiary reasons controllers are advised to resort to written consent.

3.1.3 In an employment relationship

In an employment relationship employees can be in a situation of dependence on the data controller and it needs to be checked carefully whether consent is 'freely given'.

In its Opinion WP 48, the Working Party stated that '*where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.*'

3.2 Other legal grounds for data processing

Personal data may also be processed if one or more of the following conditions are met:
- 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 before entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the data controller is subject;
- the processing is necessary to protect the data subject's vital interests;
- the processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed; or
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom

the data are disclosed, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

Processing the three special categories of personal data mentioned in section 1.3.2 above is, in principle, prohibited unless the processing meets certain specific requirements.

In particular, sensitive data may be processed if the data subject has given his explicit consent, or the processing:

- is necessary for the purposes of carrying out the obligations and specific rights of the data controller in the field of employment law;
- is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his consent;
- relates to personal data that have been manifestly made public by the data subject;
- is necessary for the establishment, exercise or defence of a right in law; or
- is carried out in the course of its legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim.

In addition, such data may be processed if the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Judicial data may only be processed:

- under the supervision of a public authority; or
- if suitable specific safeguards are provided under national law, but a complete register of criminal convictions may be kept only under the control of official authority.

The conditions for the processing of national identification numbers or any other identifiers of general application are left for the EU member states to determine.

The Working Party has clarified the legal grounds for data processing in the employment context in its Opinion WP 48.

3.3 Direct marketing and cookies

The processing of personal data for the purposes of direct marketing is subject to the general provisions of the Directive. In addition, the Directive contains a specific provision on direct marketing. In particular, data subjects have the right to object, free of charge and without any justification, to the processing of their personal data for direct marketing purposes (see also section 5.5 below). Moreover, the Directive obliges the data controller to inform the data subject of this right.

More specific provisions on direct marketing and the sending of unsolicited commercial communications are contained in the ePrivacy Directive and Directive 2000/31/EC of 8 June 2000 on certain legal aspects

of information society services, in particular electronic commerce, in the European internal market.

With regard to cookies, Article 5(3) of the ePrivacy Directive, as amended by Directive 2009/136/EC of 25 November 2009, sets two conditions for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user (eg, the use of cookies):

- the user must have consented; and
- the user must have been provided with clear and comprehensive information in accordance with the Directive, such as information about the purposes of the processing.

To obtain valid consent, the Working Party favours the use of prior opt-in mechanisms and it has stated that relying on existing browser settings cannot be considered to be valid consent (see WP 187).

3.4 Data quality requirements

Member states shall provide that personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and kept up to date; and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or for which they are further processed.

3.5 Outsourcing

When processing is carried out on his behalf, the data controller is obliged to choose a data processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

The data controller must enter into a written contract or legal act with the processor, which should stipulate in particular that:

- the data processor shall act only on instructions from the controller; and
- the security obligations incumbent on the data controller shall also be incumbent on the processor.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use as well as the use of surveillance cameras is subject to the general data protection rules.

With regard to video surveillance, in its Opinion WP 67 the Working Party specified, among others, that:

- only a limited number of natural persons should be allowed to view or access the recorded images. Whenever video surveillance is only aimed at preventing, detecting and controlling offences, two access keys (one

for the data controller and one for the police) may be used to ensure that images are only viewed by police staff rather than by unauthorised staff.
- appropriate security measures should be implemented.
- the quality of the images recorded and the training of the operators involved is fundamental.

In addition, the ePrivacy Directive prohibits listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned (subject to exemptions).

3.6.2 Employment relationship

The monitoring of email and internet use as well as the use of surveillance cameras by the employer falls within the scope of the Directive.

In its Opinion WP 48, the Working Party specified, among other things, that:
- any monitoring, especially if it is conducted on the basis of the employer's legitimate interests, must be a proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers;
- any personal data held or used in the course of monitoring must be adequate, relevant and not excessive for the purpose for which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible; and
- workers must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair processing.

4. INFORMATION OBLIGATIONS

4.1 Who

The data controller or his representative (see section 1.3.5 above) must inform the data subjects about the processing of personal data relating to them.

4.2 What

The data subject must be informed about:
- the identity of the data controller and of his representative, if any;
- the purposes of the processing for which the data are intended;
- any further information to guarantee the fair processing of the data, such as: (i) the recipients or categories of recipients of the data; (ii) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; and (iii) the existence of the right of access to and the right to rectify the data concerning him.

If the personal data have not been obtained directly from the data subject, the data controller must provide all the above information as well as information on the categories of personal data processed.

The data controller is exempt from providing the above information if:
- the data subject is already aware of it;
- providing this information proves impossible or would require a disproportionate effort; or

- recording or disclosure of the data is expressly laid down by law.

4.3 When

When the data are not obtained directly from the data subject, the information should be provided at the time the personal data are recorded, or when a disclosure to a third party is envisaged, but no later than the first time the data are disclosed. The Directive does not specify when the information should be provided if the data are obtained directly from the data subject, but generally the information should be provided at the time of the collection of the data.

4.4 How

The Directive does not specify in which form and how the information must be provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Upon request, every data subject has the right to know whether a certain data controller is processing personal data on him and if so, the categories of the personal data, the purposes of the processing and the recipients or categories of recipients to whom the data are disclosed. In addition, the data subject is entitled to receive a copy of the personal data concerned in an intelligible form and all available information as to its source.

If the personal data are used in an automated decision-making process intended to evaluate certain aspects of his personality, the data subject has the right to be informed about the logical process upon which the automated decision-making is based (see also section 5.6 below).

5.1.2 Exceptions

The right of access can be restricted in order to safeguard: (i) national security; (ii) defence; (iii) public security; (iv) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (v) an important economic or financial interest of an EU member state or of the European Union; (vi) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (iii), (iv), (v); or (vii) the protection of the data subject or of the rights and freedoms of others.

When there is no risk of breaching the privacy of the data subject, the EU member states may restrict the right of access, when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

5.1.3 Deadline

The data controller should respond without excessive delay.

5.1.4 Charges
The data controller should respond without excessive expense.

5.2 Rectification
5.2.1 Right
The data subject shall have the right to obtain from the data controller the rectification of data that are not processed in accordance with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.

5.2.2 Exceptions
The same exceptions as for the right to access apply (see section 5.1.2 above).

5.2.3 Deadline
Not specified.

5.2.4 Charges
Not specified.

5.3 Erasure
5.3.1 Right
The data subject shall have the right to obtain from the data controller as appropriate the erasure of data that are not processed in accordance with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.

5.3.2 Exceptions
The same exceptions as for the right to access apply (see section 5.1.2 above).

5.3.3 Deadline
Not specified.

5.3.4 Charges
Not specified.

5.4 Blocking
5.4.1 Right
The data subject shall have the right to obtain from the data controller as appropriate the blocking of data that are not processed in accordance with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.

5.4.2 Exceptions
The same exceptions as for the right to access apply (see section 5.1.2 above).

5.4.3 Deadline
Not specified.

5.4.4 Charges
Not specified.

5.5 Objection
5.5.1 Right
Data subjects have the general right to object to the processing of personal data relating to them based on substantial and legitimate grounds relating to their particular situation, at least in cases where the processing is based on the following legal grounds:

- the processing of data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed; or
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed.

In addition, the data subject has the right to object to the processing of personal data relating to him for direct marketing purposes (see section 3.3 above).

5.5.2 Exceptions
None.

5.5.3 Deadline
The data subject has the right to object at any time.

5.5.4 Charges
The right to object to the processing of personal data for direct marketing purposes is free of charge. The Directive does not specify if charges may be imposed to exercise the general right to object.

5.6 Automated individual decisions
5.6.1 Right
A decision producing legal effects for a data subject, or materially affecting him, cannot be taken purely on the basis of automated data processing aimed at evaluating certain aspects of his personality.

In the case of such an automated decision, the data subject has the right to be informed about the logic involved in any automated processing of data relating to him.

5.6.2 Exceptions
A person may be subjected to such an automated individual decision on condition that the decision is taken in the course of the entering into or performance of a contract, provided: (i) the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied; or (ii) that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view.

A person may also be subjected to an automated individual decision

if that decision is authorised by a law which also lays down measures to safeguard that person's legitimate interests.

5.6.3 Deadline
Not specified.

5.6.4 Charges
Not specified.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The data controller has the obligation to notify the data protection authority of any wholly or partly automatic processing operation.

6.1.2 What
The notification shall contain at least:
- the name and address of the data controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 of the Directive to ensure security of processing.

6.1.3 Exceptions
EU member states may provide for the simplification of, or exemption from, notification, in the following two cases:
- where, for categories of processing operations which are unlikely to affect adversely the rights and freedoms of data subjects, the EU member states specify: the purposes of the processing; the data or categories of data undergoing processing; the category or categories of data subject; the recipients or categories of recipients to whom the data are to be disclosed and the length of time the data are to be stored; and/or
- where the data controller has appointed a personal data protection official, responsible in particular: (i) for ensuring in an independent manner the internal application of the national provisions implementing the Directive; and (ii) for keeping the register of processing operations carried out by the data controller.

Moreover, the EU member states may exempt from notification, processing the sole purpose of which is the keeping of a register which is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating

a legitimate interest.

EU member states may also provide for an exemption from the obligation to notify, or a simplification of the notification, in the case of processing of 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, that is carried out in the course of its legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade union aim.

Finally, EU member states may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

6.1.4 When

The notification must be made before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

6.1.5 How

Not specified.

6.1.6 Notification fees

Not specified.

6.2 Authorisation requirements

Authorisation may be required for the transfer of personal data to a country which is not a member of the European Economic Area (EEA) and which does not provide an adequate level of protection (see section 8 below).

6.3 Other registration requirements

EU member states must determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to their start (so-called 'prior checking'). The prior checking must be carried out by the national data protection authority following receipt of a notification from the data controller or, where one has been appointed, by the data protection officer.

6.4 Register

EU member states must ensure that their national data protection authority holds a public register of notified processing operations. The register shall contain at least:

- the name and address of the data controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;

- proposed transfers of data to third countries.

The public register can be inspected by any person.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The Directive foresees the possibility for EU member states to simplify the notification, or be exempt from notification, for a data controller that has appointed a 'personal data protection official'. The function is not further specified in the Directive, although it follows from the preamble that such a person ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects, could be an employee of the data controller and must be in a position to exercise his functions with complete independence.

7.2 Tasks and powers

See section 7.1 above.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The transfer of personal data to a third country outside the EEA may only take place if the third country in question ensures an adequate level of protection.

The adequacy of the third country must be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration shall be given to the nature of the data; the purpose and duration of the proposed processing operation or operations; the country of origin and country of final destination; the rules of law both general and sectoral in force in the third country in question; and the professional rules and security measures which are complied with in that country.

If the European Commission, in accordance with the procedure provided for in Article 31(2) of the Directive, finds that a third country ensures an adequate level of protection, the EU member states are required to comply with the European Commission's decision.

So far, the European Commission has recognised the following countries as providing an adequate level of protection (the so-called 'white list'): Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey and Switzerland. Other countries, like Uruguay and New Zealand, are in the process of receiving adequacy recognition and may join the list.

More information can be found at: *http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm*.

8.2 Legal basis for international data transfers

Personal data may be transferred to non-adequate third countries if one or more of the following criteria are met:

- the data subject has given his unambiguous consent to the proposed transfer;

- the transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the data subject's interests between the data controller and a third party;
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary to protect the data subject's vital interests;
- the transfer is made from a register which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in that particular case;
- the transfer is authorised by the EU member state, on condition that the data controller gives adequate safeguards, for example, by concluding a data transfer agreement (see section 8.2.1 below) or adopting binding corporate rules (see section 8.2.2 below).

8.2.1 Data transfer agreements

The European Commission has the power to decide that certain standard contractual clauses offer adequate safeguards (see section 8.2 above).

So far, the European Commission has adopted three sets of standard contractual clauses:

- Two complementary sets for data transfers from data controllers to data controllers: (i) Commission Decision 2001/497/EC of 15 June 2001; and (ii) Commission Decision 2004/915/EC of 27 December 2004.

The 2001 set of clauses has been criticised, among others, because of its joint liability regime.

The 2004 set of clauses is considered to be more business-friendly and is more commonly used. The clauses do not contain a joint and several liability clause, but instead place due diligence requirements on both the data importer and the data exporter, and make each party liable only for the damages it itself caused.

- One set for data transfers from data controllers to data processors: Commission Decision 2010/87/EU of 5 February 2010, which replaced Commission Decision 2002/16/EC of 27 December 2001.

The key change introduced by the 2010 set of clauses is the possibility of sub-processing. However, the new clauses only apply to data processors based in third countries not providing adequate protection and not to EU-based data processors using sub-processors outside the EU.

The standard contractual clauses benefit from a specific favourable treatment in that the member states have to recognise them as fulfilling the requirements laid down by the Directive for the export of data and consequently may not refuse the data transfer. However, in order to benefit from this treatment, the clauses may not be amended or changed.

In addition, companies may prepare their own data transfer agreements.

However, these do not benefit from automatic recognition as providing an adequate level of protection and will be subject to the EU member states' scrutiny. This possibility is therefore rarely used.

8.2.2 Binding corporate rules

The Directive does not contain provisions concerning the use of binding corporate rules (BCRs). However, the Working Party has stated that international transfers of personal data from the EU within a group of companies can take place on the basis of BCRs. In a number of documents (WPs 155, 154, 153, 133, 108, 107, 74), the Working Party has set out a framework for the structure of such BCRs and the necessary elements to be included in them.

The BCRs need to be approved by each national data protection authority in all EU member states where a legal entity of the group will rely on them. However, the approval process has been simplified by the so-called 'mutual recognition procedure': one national data protection authority takes up the role of lead authority. Once the lead authority considers that the BCRs meet the requirements as set out in the documents of the Working Party, the data protection authorities under mutual recognition (at the moment, 19 countries are part of the mutual recognition procedure: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovenia, Spain, and the United Kingdom) accept this opinion as sufficient basis for providing their own national authorisation for the BCRs, or for giving positive advice to the body which provides that authorisation. So far the list of companies published by the European Commission for which the EU BCR mutual recognition procedure is closed only contains the names of 15 companies (the lead authorities having been the UK, the French and in one case the Luxembourg data protection authorities).

8.2.3 Safe Harbour

The Directive does not contain provisions on the EU-US Safe Harbour scheme. However, the European Commission has accepted the adequacy of this self-certification scheme in its Decision 2000/520/EC. Companies located in the US can voluntarily participate in the scheme if they adhere to the seven Safe Harbour principles:

(1) Notice.
(2) Choice.
(3) Conditions for onward transfer.
(4) Security.
(5) Data integrity.
(6) Access.
(7) Enforcement.

In addition they have to:

- disclose their private policies publicly;
- accept jurisdiction of the US Federal Trade Commission or the US Department of Transportation (sectors excluded from their jurisdiction, such as financial services, are not allowed to join the scheme); and

- notify the US Department of commerce of the self-certification.

More information can be found at: *http://safeharbor.export.gov/list.aspx*.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Any person acting under the authority of the data controller or of the data processor, including the data processor himself, who has access to personal data, must not process the data except on instructions from the controller, unless he is required to do so by law.

9.2 Security requirements

The data controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The data controller must, where processing is carried out on his behalf, choose a data processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures (see section 3.5 above).

9.3 Data security breach notification obligation

The Directive does not contain a provision on the notification of data security breaches. However, the ePrivacy Directive obliges providers of publicly available electronic communications services to notify data security breaches and the European Commission considers extending this obligation in the revised EU data protection legal framework.

9.4 Data protection impact assessments and audits

The Directive does not contain provisions on impact assessments and audits. However, the European Commission and the Working Party have recommended carrying out impact assessments, for instance, for the use of new technologies (see, eg, the European Commission's Recommendation on RFID of 12 May 2009 and WP 180) and the European Commission considers including in the revised EU data protection legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The national data protection authorities and the national courts have the power to enforce the national data protection legislation. The enforcement powers of the national data protection authorities differ from EU member state to EU member state. However, they usually include the power to investigate and to impose sanctions.

10.2 Sanctions

The Directive requires EU member states to determine the sanctions to be imposed in case of infringement of the national laws implementing the Directive.

10.3 Examples of recent enforcement of data protection rules

Not applicable.

10.4 Judicial remedies

The Directive requires EU member states to provide the right for every person to judicial remedy for any breach of this person's rights guaranteed by the national law applicable to the processing in question.

10.5 Class actions

The Directive does not provide for a right to class actions in the field of EU data protection law. However, the European Commission considers extending the power to bring an action before courts both to national data protection authorities and to other associations representing data subjects' interests in the revised EU data protection legal framework.

10.6 Liability

The Directive requires EU member states to provide that any person who has suffered damage as a result of an unlawful processing operation, or of any act incompatible with the national laws implementing the Directive, is entitled to receive compensation from the data controller for the damage suffered.

France

Sarrut Avocats Raphaël Dana & Ramiro Tavella

1. LEGISLATION

1.1 Name/title of the law

The French legal framework on data protection and privacy is provided by the Act n° 78-17 of 6 January 1978 on data processing, data files and individual liberties (*loi relative à l'informatique, aux fichiers et aux libertés*, (the DPA)), as amended, notably by the Act n° 2004-801 of 6 August 2004 (implementing the Data Protection Directive 95/46/EC).

In addition, other legal sources contain provisions on the protection of privacy and personal data including:

- the Civil Code (notably Article 9);
- the Labour Code;
- the Penal Code;
- Employment Law n° 82-689 of 4 August 1982 relating to the freedoms of employees in the work place (*loi relative aux libertés des travailleurs dans l'entreprise*);
- the law relating to security, Act n° 95-73 of 21 January 1995 (as subsequently modified by Act n° 2003-239 of 18 March 2003 and Act n° 2011-267 of 14 March 2011);
- the law n° 2011-267 of 14 March 2011, *loi d'orientation et de programmation pour la performance de la sécurité intérieure*, which has significantly changed the legal regime on video surveillance (some of these changes relate directly to the French data protection authority); and
- the deliberations and reports of the French data protection authority (the *Commission nationale de l'informatique et des libertés* or CNIL), published on the CNIL's website and on the French official website *www.legifrance.gouv.fr*, should also be taken into account.

1.2 Pending legislation

On 22 June 2011, a specific commission of the National Assembly published a report recommending that legislation be enacted:

- imposing a CNIL authorisation for geolocalisation systems;
- clarifying the legal status of IP addresses;
- implementing a 'right to online oblivion' ('*droit à l'oubli*') regarding social networks; and
- prohibiting that sensitive data be stored on cloud computing systems which are located outside of the European Union.

It remains to be seen whether this will be followed up by any legislative initiatives.

Recent and quite revolutionary is the Order n° 2011-1012 of 24 August

2011 on electronic communications, containing various provisions which aim to adapt French legislation to European Union law.

New obligations are created: electronic communication service providers are now required to handle various notifications when data security breaches occur.

The legal entities concerned are those who process personal data as part of electronic communication services provided via a public network (such as internet service providers, telecommunication companies).

This new text provides a definition of a data security breach: any tampering of the data which accidentally or unlawfully results in the destruction, loss, alteration, disclosure or unauthorised access to personal data processed in the frame of electronic communication services provided to the public.

In such a situation, the data controller concerned is now required to inform the CNIL without delay, and also the individuals concerned if the breach is likely to have adverse consequences on those individuals' right to the protection of personal data or right to privacy.

The information of the person whose personal data has been violated can be avoided if the CNIL determines that appropriate safeguards have been implemented to make the data unintelligible to any unauthorised person and that such safeguards have been applied to the data concerned. The CNIL may however, after having taken into account the gravity of the violation, request the effective notification of the individual concerned.

The companies concerned must maintain an inventory of violations (modalities, consequences) and measures taken to remedy them. Such records shall be kept for an undefined term, so they remain available to the CNIL. A company which does not comply with these provisions can be punished by up to five years imprisonment and a €300,000 fine (Penal Code, new Article 226-17-1). In addition, Order n° 2011-302 of 22 March 2011 was authorised by the government to facilitate the transposition of the amendments to the ePrivacy Directive in 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) and Directive 2009/140/EC (amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services) into French law.

1.3 Scope of the law

1.3.1 The main players

The 'data controller' means (unless expressly designated by legislative or regulatory provisions relating to the processing) a person, public authority,

department or any other organisation who determines the purposes and means of the data processing.

The 'data subject' means a natural person to whom the data covered by the processing relate.

A 'data processor', or a person who acts under the authority of the data controller, may process personal data only under the data controller's instructions. Any person who processes personal data on behalf of the data controller is regarded as a data processor.

The 'recipient' is any authorised person to whom the data are disclosed, other than the data subject, the data controller, the data processor and persons who, due to their functions, are in charge of processing the data.

1.3.2 Types of data

'Personal data' are defined by the DPA as any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

The DPA identifies other types of data.

'Sensitive data' are data that reveal, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life.

Judicial data' are data relating to offences, convictions and security measures imposed by:

(i) courts, public authorities and legal entities that manage public services, within the framework of their legal remit;
(ii) representatives of the law for the strict needs of the exercise of the functions granted to them by the law; and
(iii) legal persons acting by virtue of intellectual property rights that they administer or on behalf of victims of infringements of intellectual property rights, and for the purposes of ensuring the defence of these rights.

1.3.3 Types of acts/operations

The DPA defines the processing of personal data as any operation or set of operations in relation to such data, whatever the mechanism used, especially: the obtaining; recording; organisation; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission, dissemination or otherwise making available; alignment or combination; blocking; deletion; or destruction.

The 'material' scope of the DPA is the automatic processing of personal data as well as the non-automatic processing of personal data that is or may be contained in files, with the exception of processing carried out for the exercise of exclusively private activities.

1.3.4 Exceptions

The provisions of the DPA do not apply to temporary copies made in the

context of technical operations of transmission and access provision to a digital network for the purpose of automatic, intermediate and transitory storage of data and with the sole aim of allowing other recipients of the service to benefit from the best access possible to the transmitted information.

1.3.5 Geographical scope of application

The following situations fall within the geographical scope of application of the DPA:

- the data controller is established on French territory; or
- the data controller, although not established on French territory or in any other EU member state, uses means of processing located on French territory (except for processing used only for the purposes of transit through this territory or that of any other EU member state).

2. DATA PROTECTION AUTHORITY

National Commission on Computers and Liberties (*Commission nationale de l'informatique et des libertés*)
8 rue Vivienne, 75002 Paris, France
T: +33 1 53 73 22 22
F: +33 1 53 73 22 00
W: *www.cnil.fr*

2.1 Role and tasks

The CNIL is an independent administrative authority that protects privacy, personal data and public liberties. Its general mission is to ensure that information technology remains at the service of citizens, and does not jeopardise human identity, does not breach human rights, privacy, individual or public liberties.

Under the DPA, the CNIL has the following assignments:

- it shall inform all data subjects and data controllers of their rights and duties;
- it shall ensure that the processing of personal data is carried out in conformity with the provisions of the DPA;
- it shall keep itself informed of developments in information technology and make public its assessments of these consequences for the exercise of rights and liberties;
- in order to perform its functions, the CNIL may act by making recommendations and take individual or regulatory decisions in the cases provided for in the DPA;
- the CNIL shall present to the President of the French Republic, the Prime Minister and the Parliament an annual public report reviewing the performance of its mission.

The CNIL proposes to the government all the necessary legislative or regulatory measures to adapt the protection of rights and liberties to the evolution of technologies. It supervises compliance with the law, by inspecting information technology systems and applications. The CNIL uses

its inspection and investigation powers to investigate complaints, improve its knowledge of some specific files, better appreciate the implications of using IT in some sectors, and follow up on its deliberations.

The CNIL also monitors the security of information systems by checking that all precautions are taken to prevent the data from being distorted or disclosed to unauthorised parties.

2.2 Powers

The CNIL must authorise data processings where data are collected in the following categories: political; philosophical; medical and sexual life data; genetic data; offences; automatic processing which may, due to its nature, importance or purposes, exclude persons from the benefit of a right; automatic processing whose purpose is the combination of files; NIR (ie social security number); social difficulties; and biometrics.

It must give its opinion on data processing relating to state security and criminal offences as well as public data processing, including social security numbers, census operations, and online public services.

The CNIL also receives claims, petitions and complaints relating to the carrying out of the processing of personal data and informs the initiators of these actions of the decisions taken regarding them.

It shall respond to requests from public authorities and courts for an opinion and advise individuals and bodies that set up or intend to set up automatic processing of personal data.

It shall immediately inform the Public Prosecutor of offences of which it has knowledge and may present its views in criminal proceedings according to the conditions set out in the DPA.

The CNIL may, by specific decision, entrust one or several of its members or agents to undertake, within the limits provided for in the DPA, verifications relating to all processing and, if necessary, to obtain copies of all documents or any medium that are useful to its tasks.

It may take one of the measures provided for in the DPA (sanctions and urgent measures) against the data controller, and it shall respond to requests for access concerning processing involving state security, defence or public safety, and public processing in relation to offences and taxation.

2.3 Priorities

In its 2010 activity report published on 16 November 2011, the CNIL highlights the following topics: increasing awareness of youngsters and of teachers regarding good online surfing privacy practices (notably as regards the exposure of private life on social networks online); research and actions to be taken regarding the increasing practice of cyberbullying (repeated mockery of someone online, harassment via email, etc); the revision of the European legal framework with respect to data privacy; controls on video surveillance systems.

More generally, and as previously outlined in its 2009 annual report, the CNIL considers that the ability to understand and anticipate technological developments is essential and it has increasingly been consulted on topics

in connection with technology and the implementation of innovative information systems (eg biometric passport, electronic vote, electronic mobile bracelet).

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

The DPA does not provide a definition of consent *per se*. However, consent is generally interpreted in light of the definition contained in the Directive.

3.1.2 Form

The DPA does not require consent to be given in a specific form. However, processing sensitive data (pertaining to racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or which concern health or sexual life) requires that the data subject has given his 'express' consent.

3.1.3 In an employment relationship

The CNIL does not provide any specific information regarding the consent of employees, except in connection with the handling of social and cultural matters, usually by the Works Council, within the company.

In such a case, a specific guidebook mentions that the sending of promotional offers using the employee's email address requires the employee's prior consent.

3.2 Other legal grounds for data processing

Personal data may also be processed if one of the following conditions is satisfied:

- compliance with any legal obligation to which the data controller is subject;
- the protection of the data subject's life;
- the performance of a public service mission entrusted to the data controller or to the data recipient;
- the performance of either a contract to which the data subject is a party or of steps taken at the request of the data subject prior to entering into a contract;
- the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

The DPA provides for specific provisions regarding the processing of information for medical research, processing of personal medical data in some instances and processing of personal data for the purpose of journalism and literary and artistic expression.

3.3 Direct marketing and cookies

Direct marketing may not be undertaken using email addresses or personal data collected from public spaces or on the internet.

Such data must have been properly collected: the individuals concerned must have been informed of the future direct marketing use of their data, must give their consent, and must be given a chance to oppose such use.

In most cases, prior consent is the rule and pre-checked boxes on online forms are not acceptable in this respect. Individuals must be able to freely and easily oppose the use of their data for marketing.

The other general provisions of the DPA do apply (right to be informed of the identity of the data controller, to access the data, ask for them to be modified or deleted, etc).

The Order n° 2011-1012 of 24 August 2011 transposed the Directives 2009/136 and 2009/140 and has notably added the obligation for marketing emails to systematically include an opt-out link.

The use of cookies is governed by the DPA as amended by the Order n° 2011-1012 of 24 August 2011, which provides that any subscriber or person who uses an electronic communication network shall be informed in a clear and complete manner by the data controller or his representative of:

- the purpose of any action intended to provide access, by means of an electronic transmission, to information already stored in his electronic communication equipment, or to record information in such equipment; and
- the means by which to object to such action.

Such access or recording may only occur provided that the subscriber or the person has expressed, after having received such information, his consent, which may result from the relevant settings of his connection device or of any other device under that subscriber's or person's control.

These provisions shall not apply if the access to information stored in the terminal equipment of the user or the recording of information in the terminal equipment of the user is:

- exclusively intended to allow or facilitate communication by electronic means; or
- strictly necessary for the provision of an online communication service at the user's express request.

3.4 Data quality requirements

The DPA lays down the following requirements regarding the quality of personal data. In particular personal data shall be:

- obtained and processed fairly and lawfully;
- obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are obtained and further processed;
- accurate, complete and, where necessary, kept up to date; and
- stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.

3.5 Outsourcing

A data processor, or a person who acts under the authority of the data controller or that of the data processor, may process personal data only under the data controller's instructions.

Any person who processes personal data on behalf of the data controller is regarded as a data processor within the meaning of the DPA.

The data processor shall offer adequate guarantees to ensure the implementation of the security and confidentiality measures mentioned in the DPA. This requirement shall not exempt the data controller from his obligation to supervise compliance with such measures.

The contract between the data processor and the data controller shall specify the obligations incumbent upon the data processor with regard to protection of the security and confidentiality of the data and provide that the data processor may act only upon the data controller's instructions.

3.6 Email, internet and video monitoring

3.6.1 General rules

Any email, internet or video monitoring likely to trigger a data collection will fall within the scope of the DPA.

Besides, the provisions of the Civil Code do provide protection with respect to secret correspondence and of private life (Article 9 reads as follows: '*Everyone has the right to respect for his private life. Without prejudice to compensation for injury suffered, the court may prescribe any measures, such as sequestration, seizure and others, appropriate to prevent or put an end to an invasion of personal privacy; in case of emergency those measures may be provided for by interim order*').

With regard to video surveillance, the Act n° 2011-267 of 14 March 2011 relating to homeland security has modified the applicable rules.

One of the major changes is the scope of new powers devoted to the CNIL in this respect, which now has the power to control all the video surveillance devices installed on the French territory, including those in the public domain. The CNIL can also summon the controllers of such systems if it believes that they are violating their obligations (notification of the public, storage limit, limitations on the number of recipients of the data, etc).

The purposes for which video surveillance may now be implemented in the public domain include the fight against drug trafficking; the prevention of natural or technological disasters; assistance to individuals; and fight against fires.

3.6.2 Employment relationship

In order to comply with French law, companies must ensure that their video surveillance system is proportionate to the purposes sought. For this purpose, numerous factors must be taken into consideration, including: the number, location, direction, features and operating times of the cameras, as well as the nature of tasks performed by the persons to be subjected to video surveillance. The recording of sounds associated with images is also among the factors to be considered.

Companies have a disclosure requirement as no surveillance can be made without first informing the employees or visitors and, more generally, any person likely to be filmed by the monitoring device.

These persons must be informed by a sign posted visibly on the premises, stating that the place is under video surveillance. The sign must also include information so the individuals are made aware of how they may exercise their right to access the data recorded.

Employees' representative bodies must be consulted before a video surveillance system may be implemented on the work premises.

The recorded images may only be viewed by authorised persons who must be trained regarding the rules governing the implementation of a video surveillance system.

Professional emails may be monitored by an employer, provided the transparency requirements imposed by the Labour Code and the DPA (information to employees, information and consultation of the Works Council, declaration to the CNIL which will depend on the kind of email monitoring device installed) are satisfied.

France's Supreme Court considers that emails exchanged using the company's email system are presumed to be of a professional nature, and may therefore be freely consulted by the employer, except when they are expressly labelled as 'personal' ones (in the subject field, or in the name of the folder where they are stored).

Such privilege may be lifted in the frame of a criminal investigation, or when ordered by a court.

The CNIL recommends that the employees be given this information by the employer (eg, in an internal policy).

Monitoring internet activity is possible in the workplace, provided that the employees' representative bodies have been properly consulted and informed and the employees are made aware of the purpose of the monitoring system in place as well as about information, such as the storage limit (six months is considered as a reasonable storage period).

4. INFORMATION OBLIGATIONS

4.1 Who

The data controller or his representative is responsible for providing the information to the data subject.

4.2 What

Except where the data subject is already aware of this, the data controller must provide the following information:

- the identity of the data controller and of his representative, if any;
- the purposes of the processing;
- if applicable, whether replies to the questions are compulsory or optional, and the possible consequences for the data subject of the absence of a reply;
- the recipients or categories of recipients of the data;
- the rights of individuals in relation to the processing of data;

- when applicable, the intended transfer of personal data to a state that is not an EU member state.

4.3 Exceptions

The data controller is exempt from providing the above information when:

- the data subject has already been informed, or whenever informing the data subject proves impossible or would involve a disproportionate effort compared to the interests in the information procedure;
- if the personal data obtained are, within a short period of time, to form part of an anonymisation procedure that was recognised beforehand by the CNIL as complying with the provisions of the DPA;
- if the processing of personal data is in relation to the prevention, investigation or proof of criminal offences and the prosecution of offenders;
- if processing is carried out on behalf of the state and relating to state security, defence, or public safety, to the extent that such limitation is necessary for the observance of the purposes pursued by the processing.

4.4 When

Whenever the personal data have not been obtained from the data subject, the data controller or his representative must at the time of recording of the personal data or, if disclosure to a third party is planned, no later than the time when the data are first disclosed, provide the data subject with the information outlined above.

4.5 How

The law does not specify in which form and how the information must be provided, but if the personal data are obtained by way of a questionnaire, some of the information shall be directly mentioned in the same questionnaire.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Any natural person has the right to interrogate a data controller to know whether he is processing personal data on him. The information that the data subject has the right to receive includes:

- confirmation as to whether the personal data relating to him form part of the processing;
- information relating to the purposes of the processing, the categories of processed personal data and the recipients or categories of recipients to whom the data are disclosed;
- information relating to the transfer of personal data to a state that is not an EU member state; and
- communication, in an accessible form, of the personal data relating to him as well as any available information on the origin of the data.

When data processing involves state security, defence or public safety, the

right of access shall be exercised in accordance with the specific conditions provided for by the DPA (specific request to be formulated, investigations to be conducted, etc). The same applies when the processing is carried out by public authorities and private legal entities entrusted with a public service mission for the prevention, investigation or proof of criminal offences, or the assessment or collection of taxes.

5.1.2 Exceptions

Whenever the exercise of the right of access concerns medical personal data, the data may be disclosed to the data subject, as the person chooses, directly or through a doctor that he designates for this purpose, in conformity with specific provisions of the Code of Public Health.

Data controllers may object to requests that are obviously excessive, in particular by their number or their repetitive and systematic character.

5.1.3 Deadline

The law does not specify a particular deadline.

5.1.4 Charges

Data subjects may request a copy of their personal data and data controllers may require payment of a sum of money for the delivery of the copy, which may not exceed the cost of the copy.

5.2 Rectification

5.2.1 Right

Any individual providing proof of identity may ask the data controller to rectify his personal data.

5.2.2 Exceptions

There are no exceptions to the right to rectification.

5.2.3 Deadline

There is no deadline for the right to rectification.

5.2.4 Charges

There are no charges. The DPA provides that an individual who seeks and obtains rectification of the data about him may ask for reimbursement of the expenses corresponding to the cost of the copy mentioned in section 5.1.4 above.

5.3 Erasure

5.3.1 Right

Any data subject has the right to obtain from the data controller the blocking or deletion of the personal data relating to him.

5.3.2 Exceptions

There are no exceptions.

5.3.3 Deadline
There is no deadline.

5.3.4 Charges
There are no charges.

5.4 Blocking
5.4.1 Right
Any data subject has the right to require the blocking of any use of personal data relating to him, under the same conditions as the right to obtain deletion.

5.4.2 Exceptions
There are no exceptions.

5.4.3 Deadline
There is no deadline.

5.4.4 Charges
There are no charges.

5.5 Objection
5.5.1 Right
Any individual is entitled to object to the processing of any data relating to him on legitimate grounds.

5.5.2 Exceptions
The data subject may not object where the processing satisfies a legal obligation, or where an explicit provision of the CNIL decision that has authorised the processing expressly excludes the possibility for the data subjects to object.

5.5.3 Deadline
There is no deadline.

5.5.4 Charges
There are no charges.

5.6 Automated individual decisions
5.6.1 Right
The DPA states that no court decision involving the assessment of an individual's behaviour may be based on an automatic processing of personal data intended to assess some aspects of his personality.

No other decision having a legal effect on an individual may be taken solely on the grounds of automatic processing of data intended to define the profile of the data subject or to assess some aspects of his personality.

5.6.2 Exceptions
Neither decisions taken in the context of entering into or performing a contract concerning which the data subject had an opportunity to give his comments, nor those that meet the request of the data subject shall be regarded as taken solely on the grounds of automatic processing.

5.6.3 Deadline
Not applicable.

5.6.4 Charges
Not applicable.

5.7 Other rights
5.7.1 Right
The data subject also has the right to ask a data controller to complete and update any personal data relating to him.

5.7.2 Exceptions
There are no exceptions.

5.7.3 Deadline
There is no deadline.

5.7.4 Charges
There are no charges.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The responsibility to notify the CNIL is for the data controller.

6.1.2 What
Any automated data processing of personal data must be notified to the CNIL. The CNIL has published guidance on the notification requirements and exemptions on its website.

6.1.3 Exceptions
The followings processing operations are not subject to the notification requirement:

- processing, the sole purpose of which is to keep a register which, according to laws or regulations, is intended exclusively for public information and is open for public consultation or by any person demonstrating a legitimate interest; or
- processing carried out by an association or any other non-profit religious, philosophical, political or trade union association or body.

It should be underlined that companies which have appointed a personal data protection officer (*Correspondant Informatique et Libertés* or CIL)

registered with the CNIL are exempt from the formalities of notification for data processing, except that the appointment of the CIL has to be declared to the CNIL. The only formalities remaining with the CNIL will be those in connection with an authorisation regime or where a transfer of personal data to a state that is not an EU member state is envisaged.

6.1.4 When

Notification must be made before the start of the envisaged processing activity.

6.1.5 How

Notification may be made online on the CNIL's website, or by completing a hard copy notification form and sending it back to the CNIL. The standard notification forms are available on the CNIL's website.

A simplified declaration consists of the commitment by the declaring entity to comply with an exemption. The standard declaration is to be used when no exemption exists for the data collection at stake, and it implies describing in detail the data collection, by filling in a form.

When filed electronically in the framework of an exemption or a simplified declaration, a receipt of confirmation by the CNIL is quickly received (usually less than two weeks) and the processing may then be implemented.

The notification includes information, among others, about the name of the processing; the name and address or registered office of the data controller; the purpose(s) of the processing; and the categories of the personal data processed.

6.1.6 Notification fees

There is no notification fee.

6.2 Authorisation requirements

6.2.1 Who

Typically, the data controller has the responsibility to seek the authorisation.

6.2.2 What

Authorisation is required in the following circumstances:

- processing, whether automatic or not, relating to statistical processing, political or philosophical data;
- automatic processing of genetic data, unless carried out by physicians or biologists and necessary for preventive medicine, medical diagnosis or the administration of care or treatment;
- processing, whether automatic or not, of data relating to offences, convictions or security measures, except for those carried out by representatives of justice when necessary to carry out their task of defending data subjects;
- automatic processing which may, due to its nature, importance or purposes, exclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provision;

- automatic processing the purpose of which is the combination of files of one or several legal entities who manage a public service and whose purposes relate to different public interests;
- processing relating to data which contain the registration number of natural persons in the national register for the identification of individuals, ie, the social security number and processing that requires the consultation of this register without including the registration number of natural persons in the processing;
- automatic processing of data comprising assessments of the social difficulties of natural persons;
- automatic processing comprising biometric data necessary for the verification of an individual's identity.

6.2.3 Exceptions

The following processing operations are exempt from the authorisation requirement:

- automatic processing of genetic data carried out by physicians or biologists and necessary for preventive medicine, medical diagnosis or the administration of care or treatment;
- processing, whether automatic or not, of data relating to offences, convictions or security measures carried out by representatives of justice when necessary to carry out their task of defending data subjects.

6.2.4 When

The authorisation must usually be requested prior to commencing the data processing in question.

6.2.5 How

The request is made in French, by completing and submitting a form provided by the CNIL to the CNIL. Such form includes information on the declaring entity, the purpose of the data processing, the name of the software or of the application used, the individuals concerned, the use of specific technology (RFID, chip, video surveillance, geolocation, nanotechnology, etc), the type of data collected, including any sensitive ones (social security number, biometric or genetic data, criminal offences, health data, etc), safety measures taken to protect the system and the data. The CNIL shall issue its decision within two months from the date of receipt of the application. Where the CNIL has not given its opinion within this time limit, the application for authorisation shall be deemed to have been rejected.

6.2.6 Authorisation fees

There is no authorisation fee.

6.2.7 Other registration requirements

Not applicable.

6.3 Register

The CNIL makes available to the public the list of automatic processing that notably satisfy the formalities of notification, simplified notification and authorisation by the CNIL or authorisation by a decree in *Conseil d'Etat* (ie, decision by France's Administrative Supreme Court), with a few exceptions.

This list specifies for each processing:

- the document containing the decision to create a data processing procedure or the date of the notification of this processing;
- the denomination and the purpose of the processing;
- the identity and address of the data controller or, if he is established neither on the national territory nor in any other EU member state, that of his representative;
- the function of the person or the department where the right of access is exercised;
- the categories of the personal data processed, as well as the authorised recipients and categories of recipients to whom the data may be disclosed;
- if applicable, the planned transfers of personal data to a state that is not an EU member state.

The CNIL also makes available to the public its opinions and recommendations, and some of its decisions.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

There is no obligation to appoint an in-house or external data protection officer. A title exists, for data protection officers officially declared as such with the CNIL, and known as 'CIL', (see above).

Their appointment is not a regulatory requirement but it is encouraged by the CNIL. Additionally, since June 2009, attorneys registered with the Paris Bar may be appointed to be a company's data protection officer.

Both the CNIL and the Paris Bar encourage the appointment of attorneys as data protection officers as it shows willingness for a French legal entity to work towards compliance with the mandatory provisions of the DPA.

Since the creation of this status in 2005, more and more companies are appointing CILs; the CNIL states that nearly 7,000 organisations have appointed a data protection officer and that a quarter of the companies registered on the Paris stock exchange have done so.

7.2 Tasks and powers

Companies having appointed a data protection officer declared with the CNIL entrust them with ensuring, in an independent manner, compliance with the obligations provided in the DPA.

Such companies are exempted from the formalities of notification for data processing subject to the formality of a 'declaration' of the fact that a CIL has been appointed; the only formalities remaining with the CNIL will be those in connection with an authorisation regime or where a transfer of personal data to a state that is not a EU member state is envisaged.

The CIL shall be a person with the qualifications required to perform his duties. He shall keep a list of the processing carried out, which is immediately accessible to any person applying for access, and may not be sanctioned by his employer as a result of performing his duties. He may consult the CNIL when encountering difficulties in the performance of his duties.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Data transfers from France to other European Economic Area (EEA) member states are not subject to any additional requirements, as EEA member states are considered to provide an 'adequate level of protection'. In addition, the European Commission has recognised a number of countries to provide an adequate level of protection.

Apart from the aforementioned countries, data transfers abroad are in principle prohibited, subject to exceptions.

8.2 Legal basis for international data transfers

The DPA provides that there may be an exception to the prohibition of transferring personal data outside the European Union where the process guarantees a sufficient level of protection of the individuals' privacy as well as their liberties and fundamental rights and in particular regarding contractual clauses or internal rules relating to the process.

8.2.1 Data transfer agreements

Data transfers on the basis of data transfer agreements are permitted but subject to prior authorisation from the CNIL for the transfer of personal data to states that do not provide a sufficient level of protection of individuals' privacy, liberties and fundamental rights with regard to the actual possible processing of their personal data. The European Commission's standard contractual clauses for data transfers are commonly used.

8.2.2 Binding corporate rules

The CNIL has approved the use of binding corporate rules (BCRs), but states that BCRs should not be considered as the only or best tool for carrying out international transfers but only as an additional one, where the use of existing instruments seems to be particularly problematic.

A company wishing to implement BCRs first needs to appoint a coordinating authority who will be in charge of coordinating the procedure with the other authorities involved, to whom the requests for authorisation for transfer on the basis of the BCRs will be filed.

France is part of the mutual recognition procedure and the CNIL's international and European affairs service is the contact for information and assistance in this respect.

8.2.3 Safe Harbour

There is no need for authorisation where the personal data are transferred

to an organisation that is certified under the US Safe Harbour scheme and the data transfer falls within the scope of that certification. However, the fact that the data transfer is made to a US Safe Harbour certified organisation must be mentioned in the notification to the CNIL.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The data processor and data controller shall offer adequate guarantees to ensure the implementation of the security and confidentiality measures.

9.2 Security requirements

The data controller and the data processor shall take all useful precautions, with regard to the nature of the personal data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties.

On its website, the CNIL makes available for download a report on Information Security (IS) which provides recommendations concerning the safety of personal data.

9.3 Data security breach notification obligation

The DPA does not provide for a general data security breach notification obligation. For information on the data breach notification obligation created by the Order No. 2011-1012 of 24 August 2011, only applicable to companies in the communication sector, please refer to section 1.2 above.

9.4 Data protection impact assessments and audits

There is no general requirement to carry out data protection impact assessments and audits as such under French law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The CNIL can, on its own initiative or following a complaint by an individual, carry out an audit on the spot concerning any file.

The CNIL may issue a warning to a data controller who does not comply with the obligations resulting from the DPA. It may also give a formal notification to the data controller to stop the failure of the DPA.

10.2 Sanctions

If the data controller does not comply with an order by the CNIL, the CNIL may impose the following penalties on him, after fair proceedings:

- a financial penalty, except in cases where the processing is carried out by the state;
- an injunction to stop the processing.

In terms of fines for violating the DPA, the CNIL can issue sanctions against data controllers that do not comply with the law ranging from warnings and injunctions, to levying fines.

The fines issued are proportional to the gravity of the breaches committed

and the profits obtained from the breach. In the case of a first breach, the penalty may not exceed €150,000. In the event of a second breach within five years from the date on which the preceding financial penalty becomes definitive, it may not exceed €300,000 or, in the case of a legal entity, five per cent of gross turnover for the latest financial year, with a maximum of €300,000.

All fraudulent, unfair or illegal collection of data is prohibited. Violation is governed under the Criminal Code and is punishable by five years' imprisonment and a €300,000 fine.

10.3 Examples of recent enforcement of data protection rules

In 2010 the CNIL carried out 308 verifications of data processing activities, and 111 summons letter (*CNIL 2010 Annual Activity Report*).

On 17 March 2011, the CNIL's sanctions committee issued a fine of €100,000 against Google as it had not responded to the CNIL's request in a timely manner. The CNIL had conducted a series of on-site inspections to examine the conformity of Google's collection of wi-fi data and content data (identification information, passwords, login details, email exchanges) without the knowledge of the data subjects for the purposes of its location-based services (including Google Maps, Street View and Latitude). In May 2010, the CNIL formally asked Google to rectify this situation but Google did not respond in time.

10.4 Judicial remedies

In the case of serious and immediate violation of the human identity, human rights, privacy, or individual or public liberties, the chairman of the CNIL may ask, in summary proceedings, the competent jurisdiction to order – if necessary applying a daily penalty – any security measure necessary for the protection of these rights and liberties.

The public prosecutor shall inform the chairman of the CNIL of any legal proceedings in connection with breaches related to data privacy and, when appropriate, the decisions taken in respect of them. He shall inform him of the date and purpose of the court hearings by a registered letter with advice of delivery sent at least 10 days before that date.

The judges in charge of the investigation or of the judgment of a case may request the chairman of the CNIL or his representative to submit his comments or to present them orally before the court.

As is illustrated by available case law, individuals may also file legal action before courts on the grounds of a breach of the provisions of the DPA.

10.5 Class actions

Class actions *per se* are not possible in France.

10.6 Liability

The data controller shall be held liable for any damage as a result of an action in violation of the provisions of the DPA. Data subjects who have incurred damage from an action in violation of the DPA may claim damages

from the data controller, based on the Civil Code. As is illustrated by available case law, the data controller shall be exempt from liability if he proves that the act which caused the damage cannot be ascribed to him.

Germany

Van Bael & Bellis Monika Kuschewsky

1. LEGISLATION

1.1 Name/title of the law

The Data Protection Directive 95/46/EC (the Directive) was implemented in Germany primarily by amending the Federal Data Protection Act (*Bundesdatenschutzgesetz*) (BDSG) of 1977 (in addition, each of the 16 German federal states or *Länder* has also adopted its own data protection law). The amendments entered into force on 23 May 2001. The BDSG was last amended in 2009.

Data protection is given a high level of protection under the German Constitution. The German Constitutional Court has recognised a so-called right to informational self-determination, which is the right of the individual to determine in principle himself the disclosure and use of his personal data, as well as the right to confidentiality and integrity in information technology systems. Any limitations to these rights must be based on a specific and clear law.

In addition to the BDSG, data protection rules are also contained in other laws, such as:

- the Social Act X (*Sozialgesetzbuch X*) (SGB X);
- the Telemedia Act (*Telemediengesetz*) (TMG); and
- the Telecommunications Act (*Telekommunikationsgesetz*) (TKG).

Collective bargaining or works council agreements may also contain rules on data protection.

1.2 Pending legislation

German data protection law has undergone important changes in the last couple of years and is likely to undergo further changes. Several legislative initiatives which would amend the BDSG are currently pending before the German parliament. Most significantly, the draft bill on employee data protection adopted by the German government in 2010 would amend the BDSG by introducing very detailed provisions regarding the processing of employees' personal data.

In December 2010, the German Federal Interior Minister presented a draft law which aims to enhance individuals' control over their personal data on the internet and to protect the fundamental right to protect one's personal life. This draft law still has to be formally adopted by the German government and then go through the legislative process.

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the 'e-Privacy Directive') has been implemented in

Germany by the TKG. In order to implement the changes brought about by Directive 2009/136/EC, which amended the e-Privacy Directive, the German government adopted a draft Act, which still has to go through the legislative process (see also section 3.3 below).

The German *Land Hessen* has initiated a proposal for a draft law amending the TMG which would introduce additional data protection rules applicable to certain internet services, such as social online networks.

1.3 Scope of the law

The BDSG applies to the collection, processing and use of personal data by private bodies, including natural and legal persons, companies and other private-law associations, as well as by public authorities and bodies both at federal and, to a limited extent, at *Länder* level and the rules applicable to both sectors differ. The following sections only deal with the rules applicable to the private sector.

1.3.1 The main players

- The 'data controller' is any person or body which collects, processes or uses personal data on his own behalf or which commissions others to do so on his behalf.
- The 'data processor' is any natural or legal person (but not an employee of the data controller) who collects, processes or uses personal data on behalf of the data controller.
- The 'data subject' is any natural person that is identified or identifiable in relation to personal data.
- 'Recipient' shall mean any person or body to whom or which data are disclosed. 'Third party' is any person or body other than the data controller, but not the data subject or data processors collecting, processing or using personal data in Germany, in another member state of the EU or the European Economic Area (EEA).

1.3.2 Types of data

The BDSG only covers personal data relating to natural persons.

'Personal data' are defined as 'any information concerning the personal or material circumstances of an identified or identifiable natural person (the data subject)' and include an individual's name, photograph, telephone number, bank account number, etc.

Special categories of data (sensitive data), which include information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life are subject to a stricter regime.

Once personal data have been anonymised in such a way that particulars about the personal or material circumstances can no longer, or only with disproportionate effort in terms of time, cost and work, be attributed to an identified or identifiable human being, they are no longer considered to be personal data.

1.3.3 Types of acts/operations

The BDSG applies to the automatic processing of personal data by means of a data processing device (such as a personal computer). Non-automatic processing (or manual processing) is also regulated by the BDSG, provided the personal data are recorded in a paper filing system which is structured in a similar manner in such a way that the personal data are accessible and assessable according to certain criteria (such as a card index). Paper files or records are not normally covered by the BDSG, except personnel files of employees or where the personal data have been obtained from automatic processing (such as print-outs from an electronic database).

The BDSG distinguishes in particular the following three processing categories:

- 'Collection' is the gathering of data on the data subject.
- 'Processing' is the recording, alteration, transfer, blocking and erasure of personal data and the BDSG defines each of these terms separately.
- 'Use' is any utilisation of personal data other than processing.

All the aforementioned operations are hereafter collectively referred to as 'processing'.

1.3.4 Exceptions

The BDSG does not apply to personal data processed by a private body exclusively for the purposes of personal or family affairs.

1.3.5 Geographical scope of application

The BDSG applies to the data collection, processing and use of personal data by any data controller established in Germany.

If the data controller is established neither in Germany nor in any other EEA state, the BDSG applies, if the data controller collects, processes or uses personal data in Germany otherwise than merely for the purposes of transit through Germany. Where a data controller falls under this latter provision, whenever he must inform data subjects of the identity of the data controller, he must also provide the identity of a representative in Germany.

The BDSG does not apply where a data controller established in another EEA state processes personal data in Germany, unless such operation is carried out by an establishment in Germany.

1.4 Particularities

The competence for data protection is split between federal and *Länder* level. The BDSG applies to data processing carried out by private organisations as well as to data processing carried out by public bodies at federal level and, to a limited extent, at *Länder* level, whereas the data processing of public authorities at *Länder* level is governed by the data protection laws of the 16 German *Länder*.

2. DATA PROTECTION AUTHORITY

Because of Germany's federal structure, there are data protection authorities both at federal and *Länder* level. The processing of personal data by private

bodies and organisations (with the exception of the telecommunications and postal services sector) is supervised by the supervisory authorities responsible for the protection of personal data at *Länder* level. There is such an authority in each *Land*.

The processing of personal data by public bodies on the other hand is supervised by the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) (BfDI) at federal level (who is also in charge of telecommunications and postal services companies) and at *Länder* level by the *Länder* data protection authorities. In some federal states, these latter authorities are different from the supervisory authorities that are competent for non-public bodies.

The supervisory authorities at *Länder* level are currently undergoing some organisational restructuring in reaction to a judgment rendered by the EU's Court of Justice in March 2010. In 2007, the European Commission had initiated an infringement procedure against Germany, criticising the fact that the *Länder* supervisory authorities would not be independent within the meaning of the Directive. In March 2010, the European Court issued its judgment, holding that Germany had failed to fulfil its obligations under the Directive and in particular had incorrectly transposed the requirement that the supervisory authorities perform their functions 'with complete independence' as the supervisory authorities were subject to state scrutiny.

The supervisory authorities of the German *Länder* meet regularly in the so-called *Düsseldorfer Kreis* or circle for information and experience exchange, in which they informally coordinate their activities. The most important results of their meetings are published in the form of solutions.

The contact details for all the supervisory authorities are available at the website of the BfDI.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Husarenstraße 30, D-53117 Bonn
T: +49 (0)228 99 7799 0
F: +49 (0)228 99 7799 550
E: poststelle@bfdi.bund.de
W: *www.bfdi.bund.de*

2.1 Role and tasks

The supervisory authorities monitor and enforce the provisions of the BDSG and other data protection rules governing the processing of personal data. They advise and support the data protection officers (see section 7 below) and data controllers.

The supervisory authorities publish regularly, and at least biannually, an activity report. They also deal with complaints and keep a register of all notifiable automatic data processing (see section 6.4 below).

2.2 Powers

The supervisory authorities may request information, enter property and business premises during business hours and carry out checks and

inspections. They may inspect business documents, recorded data and data processing programmes. The persons required to provide information shall allow these measures. The bodies subject to monitoring and the persons responsible for their management shall provide the supervisory authority, on request and without delay, with the information necessary to perform its duties, except where the person required to provide information would expose himself to the risk of criminal prosecution or proceedings under the Administrative Offences Act (OWiG).

Where there has been a breach of the BDSG, the supervisory authorities are empowered to inform the data subjects concerned, to report the breach to the bodies responsible for prosecution or punishment and, in the case of serious breaches, to notify the competent trade supervisory authorities (*Gewerbeaufsichtsbehörden*).

The supervisory authorities may also require data controllers to take specified steps or measures or certain technical or organisational security measures to remedy breaches of the BDSG or technical or organisational defects. In the case of serious violations or problems, they may even prohibit the collection, processing or use of personal data or the use of particular procedures, if the breaches or problems are not duly remedied within a reasonable time despite orders and the imposition of a fine. They may also demand the dismissal of a data protection officer, if he does not have the necessary specialised knowledge and reliability to perform his duties.

The supervisory authorities may also impose administrative fines for a breach of the BDSG.

For supervisory purposes, they may transfer data to other supervisory authorities. On request, they shall provide administrative assistance to the supervisory authorities of other EU member states.

The powers of the BfDI are laid down in specific provisions in the BDSG and are more limited than those of the supervisory authorities at *Länder* level. For instance, the BfDI cannot impose sanctions.

2.3 Priorities

The priorities in 2010 were issues relating to the internet as well as new technologies. One of the hot topics was the controversial Google Street View service, notably the revelation that Google had captured personal data from Wi-Fi networks with its Street View vehicles. In addition to panoramic services, the supervisory authorities also dealt with questions concerning new technologies in general, such as social networks, smart meters, geo-location data, cloud-computing services, smart phones, web analysis programmes and behavioural advertising. Other issues on which the German supervisory authorities focused concerned direct marketing and the use of personal data by address brokers, insurance companies and banks. Employee data protection, including CCTV surveillance, is always high on the authorities' agenda as are questions related to international data transfers. In 2010, the supervisory authorities were also busy advising on the impact and interpretation of the amended BDSG.

3. LEGAL BASIS FOR DATA PROCESSING

In principle, the processing of personal data is admissible only if permitted or prescribed by the BDSG or another law, or if the data subject has given his consent.

The BDSG contains special provisions relating to the use of personal data subject to professional secrecy, by research institutions and by the media. There are also specific provisions for so-called automated retrieval procedures.

3.1 Consent

The BDSG does not contain a definition of 'consent', which is however defined in the German Civil Code as prior approval. Moreover, consent is only valid if it is freely given, which basically means that the data subjects must have a real choice and be able to withhold or subsequently withdraw their consent without any negative consequences.

3.1.2 Form

Consent must be given on an informed basis. For this purpose, the data subject must be informed of the purpose of collection, processing or use, and, as the case may be or upon request, of the consequences of a refusal to give consent.

Where sensitive data are processed, the consent must specifically refer to the sensitive data.

Consent shall be given in writing, unless special circumstances warrant another form. If consent is to be given together with other written declarations, the consent must be distinguished or particularly highlighted.

The BDSG also contains specific form requirements where the consent is given for the purposes of advertising or trading in addresses.

3.1.3 In an employment relationship

The German data protection authorities usually do not consider consent to constitute a valid legal basis for the processing of employees' personal data. In their view, in most cases the employees' consent will not be freely given, as the employment relationship is characterised by subordination. Moreover, it would be misleading to seek to legitimise data processing through consent, if the processing is a necessary and unavoidable consequence of the employment relationship.

3.2 Other legal grounds for data processing

If the data processing cannot be based on consent, it is nevertheless lawful if it is permitted or required under another law or if one of the criteria mentioned in the BDSG is met.

The BDSG contains a complex set of rules for the processing of personal data. Specific rules apply where a data controller transmits personal data to rating agencies, in the case of scoring, as well as for the commercial data collection and recording for the purpose of transfer (including in anonymous form) or market and opinion research.

The data collection, storage, modification, disclosure or use of personal data for the data controller's own purposes will be lawful if:

1) the processing is necessary for the creation, performance or termination of a contract or quasi-contractual fiduciary relationship to which the data subject is a party;
2) the processing is necessary in order to safeguard the legitimate interests of the data controller and there is no reason to assume that the data subject has an overriding legitimate interest in his personal data being excluded from the processing or use; or
3) the personal data are generally accessible or the data controller would be entitled to publish them, unless the data subject's legitimate interest in his personal data being excluded from the processing clearly outweighs the legitimate interest of the data controller.

The specific purposes for which the personal data will be processed have to be established prior to the collection of the personal data.

The personal data may subsequently only be transmitted or used for other purposes in case of items 2) or 3) above or if:

- the transmission or processing is necessary to protect the legitimate interests of a third party;
- it is necessary to prevent threats to state or public security or for the prosecution of criminal offences; or
- in certain cases of scientific research, advertising or market or opinion surveys.

The BDSG contains a specific provision regarding data collection, processing and use for employment-related purposes, which basically summarises the principles which have been developed in case law. Personal data of an employee may only be collected, processed or used for the purposes of the employment relationship, if this is necessary for a decision about the creation of an employment relationship or the performance or termination of one. For the detection of criminal actions, personal data of an employee may only be collected, processed or used, if there is a documented factual reason to believe that the employee has committed a crime, the collection, processing or use is necessary to detect the crime and the employee has no overriding legitimate interest against the collection, processing or use. The rights of participation of employee representatives remain unaffected.

Personal data recorded exclusively for the purposes of monitoring data protection, safeguarding data or ensuring the proper operation of a data processing system may only be used for these purposes.

Sensitive data may only be collected, processed or used for the data controller's own purposes if the data subject has given his explicit consent or:

- if it is necessary to protect vital interests of the data subject or of a third party, provided the data subject is for physical or legal reasons incapable of giving his consent;
- if they concern personal data which have evidently been made public by the data subject;

- if it is necessary for the establishment, exercise or defence of legal claims and there is no reason to assume that the legitimate interest of the data subject in not having his personal data processed outweighs this need;
- for scientific research, subject to conditions; or
- for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services and the data are processed by health professionals subject to professional secrecy.

The sensitive data may subsequently only be transmitted or used for other purposes in one of the five aforementioned cases or if it is necessary to prevent significant threats to the state and public security or for the prosecution of criminal offences of significant importance.

3.3 Direct marketing and cookies

The BDSG contains a complex set of rules applicable to processing and use of personal data for the purpose of direct marketing. In principle, personal data may only be processed or used for direct marketing if the data subject has given his consent; besides, the processing or use may also be allowed if only a limited set of data from lists is processed under certain conditions. As the rules have recently changed, the amended BDSG includes provisions for the transition and in some cases the new rules will only take effect at the end of August 2012.

If the data subject lodges an objection to the processing or use of his personal data for direct marketing purposes, the processing or use of his data for these purposes shall be unlawful. In certain cases the personal data shall be blocked. The data subject shall be informed of the identity of the data controller and the right to object, as well as in certain cases, the source of the data (see also section 5.5 below).

The TKG contains specific rules regarding direct marketing in the telecommunications sector and the TMG provides for special information obligations regarding unsolicited electronic commercial communications. Other laws, such as the Law on Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*), which requires, in most cases, the consent of the recipient for direct marketing by telephone, email and fax, might also apply.

Germany has not yet implemented the amended e-Privacy Directive, including the so-called cookie clause. The draft law for the implementation of the e-Privacy Directive presented by the German government expressed the opinion that the current German law does not need to be amended with respect to the cookie clause. Rather the German government wanted to wait for the outcome of the ongoing discussions at European level as to the interpretation of the cookie clause, including the self-regulatory attempts by the industry, before proposing any new legislative measures. The German supervisory authorities on the other hand have called upon the German government to take legislative action. In their view the current law does not reflect the amended version of the e-Privacy Directive, as it provides for a right to object rather than for informed consent, which is required by the cookie clause of the amended e-Privacy Directive. It is reported that the

German government is currently examining how the cookie clause may be implemented by a provision in the TMG and will make a proposal in the framework of the reform of the TKG.

3.4 Data quality requirements

The BDSG puts a particular emphasis on the so-called data reduction and data economy principles (also called data minimisation principle). These require data processing systems to be selected and designed in accordance with the aim of processing as little personal data as possible. In particular, use is to be made of the possibilities for anonymising (see section 1.3.2 above) or pseudonymising (replacing a person's name and other identifying characteristics with another identifier in order to make it impossible or extremely difficult to identify the data subject), in so far as this is possible with respect to the purpose for which the data are collected and/or further processed and the effort involved is not disproportionate in relation to the desired purpose of protection.

In principle, personal data should be obtained directly from the data subject. Personal data may only be collected without the data subject's participation if this is provided for in, or mandatory under, a law; the administrative task or the business purpose require a collection from other persons or organisations; or the collection from the data subject would require a disproportionate effort and there are no indications that overriding legitimate interests of the data subject would be adversely affected.

3.5 Outsourcing

Where the processing of personal data is carried out by a data processor on behalf of the data controller, the data controller remains responsible for compliance with the BDSG and other data protection rules. The data controller shall carefully choose a data processor with special attention to the suitability of the technical and organisational measures taken by the data processor. There must be a written agreement in place between the data controller and the data processor which must lay down:

- the subject matter and duration of the work to be carried out;
- the extent, type and purpose of the intended data collection, processing or use, the type of data and the category of data subjects;
- the technical and organisational measures to be taken;
- the rectification, erasure and blocking of data;
- the data processor's obligations, in particular monitoring;
- any right to subcontract;
- the data controller's rights to monitor and the data processor's corresponding obligations to tolerate and cooperate;
- those violations by the data processor or its employees of either provisions to protect personal data or of the terms specified by the data controller which are subject to the obligation to notify;
- the extent of the data controller's authority to issue instructions to the data processor; and
- the return of data storage media and the erasure of data recorded by the

data processor after the work has been carried out.

The data processor may collect, process or use the data only as instructed by the data controller. If he believes that an instruction by the data controller violates the BDSG or other data protection rules, he shall inform the data controller immediately. Data processors are also subject to the confidentiality obligation (see section 9.1 below) and the obligation to take technical and organisational security measures (see section 9.2 below).

The same rules apply by analogy where automatic data processing operations or systems are checked or maintained by other parties on the data controller's instructions and it cannot be excluded that the personal data may thereby be accessed.

If the data processor is established outside the EEA, he is considered a third party and, in addition to respecting the aforementioned rules regarding data processors, the data controller must also ensure that the data transmission can be based on one of the legal grounds for making data processing legitimate (see sections 3.1 and 3.2 above).

3.6 Email, internet and video monitoring

3.6.1 General rules

The BDSG does not contain any specific provisions regarding email and internet monitoring; rather, the general rules apply.

Video monitoring by private bodies in publicly accessible spaces is only admissible when it is either necessary for the exercise of the right to determine who shall be allowed or denied access or to pursue legitimate interests for specifically defined purposes, and provided that there are no indications of overriding legitimate interests of the data subject. The monitoring as well as the identity of the data controller must be made visible. The recorded personal data may only be processed or used for other purposes, if this is necessary to prevent threats to state and public security or to prosecute crimes. The data shall be erased immediately as soon as they are no longer necessary to achieve the purpose or further storage would conflict with the legitimate interests of the data subject.

3.6.2 Employment relationship

Where the employer has allowed his employees to use business email and internet for private purposes, the specific rules of the TKG, and in particular the telecommunications secrecy, apply. This basically means that in such a case the employer is not entitled to access the content of any emails, be it business or private emails, and has to obtain consent from the employees to monitor their emails and internet use. A breach of the telecommunications secrecy may be punished with imprisonment.

In order to avoid the application of the TKG and in particular the telecommunications secrecy, some employers have therefore prohibited the use of their emails and internet for private purposes. However, it should be noted that even if consent has been obtained, any monitoring will still be subject to general data protection principles. Employers should also set out details of the monitoring in clear terms in internal guidelines and policies.

The use of any monitoring techniques, including video monitoring, ultimately requires a balancing of the rights of the employees to their personal lives with the interest of the employer, whereby the obligation of the employer to safeguard his employees must be taken into account.

The new draft bill on employee data protection proposes a specific provision for video monitoring of employees which would limit the purposes for which such monitoring can be undertaken as well as set out the conditions for such monitoring. The new draft bill also proposes a specific provision for the use of geo-location data of employees.

4. INFORMATION OBLIGATIONS

The BDSG distinguishes between two scenarios, namely where personal data are processed and used for own purposes and where personal data are recorded on a commercial basis for the purpose of transfer. The applicable rules differ slightly and this section only deals with the first scenario.

4.1 Who

Data controllers are responsible for providing information to the data subjects about the processing of personal data relating to them.

4.2 What

If personal data are collected from the data subject, he must be informed about:

- the identity of the data controller;
- the purpose of the collection, processing or use; and
- the categories of recipients in so far as the data subject need not expect that his personal data will be transmitted to such recipients.

Where the data subject is obliged by law to provide the information or the information is a prerequisite for granting legal benefits to the data subject, the data subject must be informed that the supply of the information is obligatory or voluntary, as the case may be. In so far as the circumstances of the individual case dictate, or at his request, the data subject shall also be informed of the legal provision obliging him to provide the information and of the consequences of withholding particulars.

If personal data are stored for the first time for the data controller's own purposes without the data subject's knowledge, in addition to the information above, the data subject must also be informed about the fact of the storage.

No information has to be provided to the data subject in the latter case if, for instance:

- the data subject has already acquired knowledge of the storage;
- the personal data are only recorded, because they may not be erased due to retention obligations under law, articles of association or contracts or the personal data only serves the securing or monitoring/control of data and informing the data subject would involve a disproportionate effort;
- the personal data have to be kept confidential;
- the recording is prescribed by law; or

- the recording is necessary for the purposes of scientific research and notification would require a disproportionate effort.

The data controller shall lay down in writing the conditions under which he may refrain from informing the data subject(s).

4.3 When

If the data are collected from the data subject, the data subject shall be informed at the time of the collection. The BDSG does not specify when the information has to be provided where the personal data are recorded for the first time without the data subject's knowledge.

4.4 How

The BDSG does not specify in which form and how the information must be provided.

5. RIGHTS OF INDIVIDUALS

The rights of the data subjects may not be excluded or limited by contract. The BDSG distinguishes between two scenarios and the applicable rules differ slightly: the personal data are processed and used for the data subject's own purposes or the personal data are collected and recorded on a commercial basis for the purpose of transfer. This section only deals with the first scenario. Moreover, specific rules apply to certain forms of advertising.

5.1 Access

5.1.1 Right

Data subjects may request information about recorded data relating to them, including information relating to the source of the data, the recipients or categories or recipients to whom the data are disclosed, and the purposes of the recording. The data subject shall specify the type of personal data to which he requires access. The data subject shall be informed by the data controller in writing, unless another format is more appropriate in the circumstances concerned.

5.1.2 Exceptions

The data controller does not have to inform the data subject if, for instance:

- the personal data are only recorded, because they may not be erased due to retention obligations under law, articles of association or contracts or the personal data only serve the securing or monitoring/control of data and informing the data subject would involve a disproportionate effort;
- the personal data must be kept confidential; or
- the recording or transmission is necessary for the purposes of scientific research and notification would require a disproportionate effort.

5.1.3 Deadline
The BDSG does not specify any deadline within which the right to access must be granted.

5.1.4 Charges
The right to access is free of charge.

5.2 Rectification
5.2.1 Right
Personal data must be rectified if they are incorrect. Estimated data must clearly be marked as such. If the data were disclosed to others for recording, the data controller must inform the recipients, if this does not require a disproportionate effort and this does not conflict with the legitimate interests of the data subject.

5.2.2 Exceptions
There are no exceptions to the right to rectification.

5.2.3 Deadline
The BDSG does not specify any deadline within which this right must be granted.

5.2.4 Charges
The right to rectification is free of charge.

5.3 Erasure
5.3.1 Right
Personal data may be deleted any time, unless this is contrary to the retention periods provided for by law, articles of association or a contract or there is reason to assume that the deletion would affect the legitimate interests of the data subject.

Personal data must be deleted if:

- their recording is inadmissible;
- they concern sensitive data or data about criminal acts or offences and the data controller cannot prove the accuracy of the data; or
- the data are processed for the data controller's own purposes and are no longer needed for the purpose concerned.

5.3.2 Exceptions
There are no exceptions to the right to erasure.

5.3.3 Deadline
The BDSG does not specify any deadline within which this right must be granted.

5.3.4 Charges
The right to erasure is free of charge.

5.4 Blocking

5.4.1 Right

Instead of being deleted, access to the personal data must be blocked if:

- their recording is inadmissible, but holding the data is required by law, articles of association or a contract;
- there is reason to assume that their deletion would affect the data subject's legitimate interests;
- deletion is impossible due to the particular kind of recording or is only possible involving disproportionate efforts; or
- the data subject contests the data's correctness, but it can neither be proven that the data are correct nor that they are incorrect.

Without the data subject's consent, blocked data may only be transmitted or used if they are indispensable for scientific purposes; necessary to improve a situation which lacks evidence; or are indispensable for other reasons following from the data controller's or a third party's interests that outweigh the data subject's interest and the data could be transmitted or used for this purpose, if they were not blocked.

5.4.2 Exceptions

There are no exceptions to the blocking right.

5.4.3 Deadline

The BDSG does not specify any deadline within which the blocking right must be granted.

5.4.4 Charges

The blocking right is free of charge.

5.5 Objection

5.5.1 Right

The data subject is entitled to object to the processing of his personal data in automatic form or in non-automatic filing systems if the data subject lodges an objection with the data controller and an examination indicates that the data subjects' legitimate interests outweigh the interest of the data controller to collect, process or use the data, taking into account the data subject's special personal situation.

In addition, the data subject has the right to object to the processing of personal data relating to him for direct marketing purposes and market research and opinion polls and must be informed about this right when he is approached for the purpose of advertising or in some cases when entering into a contract or similar relationship. The data subject may also exercise this right *vis-à-vis* third parties, in which case the third party must block the personal data for these purposes.

5.5.2 Exceptions

The data subject does not have the general right to object if the processing is required by law.

No exceptions apply with respect to the right to object to the processing of personal data for direct marketing purposes.

5.5.3 Deadline

The data controller must stop the processing of personal data upon the data subject's objection.

5.5.4 Charges

The right to object is free of charge.

5.6 Automated individual decisions

5.6.1 Right

Decisions, which have legal consequences for the data subject or may significantly affect him, may not be exclusively based on the automatic processing of personal data which serves the evaluation of individual characteristics of his personality. This is, for instance, the case if there has been no involvement by a natural person.

In addition, the data subject has the right to be informed by the data controller of the logic involved in the automatic processing of his personal data.

5.6.2 Exceptions

The right is subject to the following exceptions:

- the decision is made in the framework of the conclusion or performance of a contract or other legal relationship and grants a request made by the data subject; or
- the legitimate interests of the data subject are safeguarded by appropriate means and the data controller has communicated to the data subject the fact that an automated decision has been involved and, upon request, communicates and explains the essential reasons for this decision.

5.6.3 Deadline

The BDSG does not specify any deadline within which the blocking right must be granted.

5.6.4 Charges

The data subject may not be charged for exercising this right.

5.7 Other rights

Anybody who believes their rights have been violated through the collection, processing or use of their personal data by federal public bodies may complain to the BfDI. The data protection laws of the *Länder* lay down similar rights to complain to their data protection authorities against actions by state public authorities.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The responsibility for the notification with the competent supervisory authority lies with the data controller. In practice, the general notification obligation applies to small and medium-sized organisations that are not obliged to appoint a data protection officer. However, these organisations often lack the awareness and resources for data protection compliance and the number of registrations is rather low. For instance, in 2007 and 2008 the supervisory authority in Hessen, one of the 16 *Länder* , which is one of the most financially well-off regions in Germany, received a total of 120 notifications from 104 data controllers. In Bavaria, 138 notifications were made in 2009/2010.

6.1.2 What

In principle, every data controller who is processing personal data in an automatic manner is required to notify the competent supervisory authority prior to commencing the processing operation, unless the data processing falls under one of the exemptions.

A specific registration regime applies to data storage for the purposes of commercial disclosure/transmission to third parties, ie, trading personal data, eg, by credit agencies and address brokers, as well as data storage for the purposes of anonymous disclosure/transmission to third parties and for market research and opinion surveys. The following section only deals with the general notification regime.

6.1.3 Exceptions

There is no need to notify if: (i) either the data controller has appointed a data protection officer (see section 7 below); or (ii) the data controller collects, processes or uses the personal data for his own purposes and as a rule deploys for this purpose permanently a maximum number of nine employees and either consent has been obtained from the data subject or the processing is required for the conclusion, performance or termination of a contract or a quasi-contractual fiduciary relationship with the data subject.

6.1.4 When

Notification must be made prior to commencing the processing operation.

The notification does not have to be renewed. However, a new notification has to be made where there is any subsequent change to the information that was contained in a notification or where the processing is terminated.

6.1.5 How

The notification has to be sent to the competent supervisory authority. There is no uniform standard notification form. However, some supervisory authorities publish notification forms on their website. Notification may be made by completing a notification form, if any, or providing the required

registrable particulars in writing, namely:

- the data controller's name and address;
- the owners, board members, managers or other persons managing the company and the persons entrusted with the management of data processing;
- the name and address of a representative in Germany, if the data controller is not established in the EEA;
- the purpose(s) of the data collection, processing or use;
- a description of the category or categories of data subjects and the personal data or categories of personal data relating to them;
- a description of the recipient(s) or categories of recipients;
- the usual periods for erasing the personal data;
- envisaged transfers of personal data to third countries; and
- a general description of the technical and organisational security measures allowing a preliminary assessment of their appropriateness.

6.1.6 Notification fees

There is no notification fee.

6.2 Authorisation requirements

In principle, data controllers do not need to obtain authorisation to carry out a data processing activity. However, some German supervisory authorities used to take the view that even an international data transfer based on the European Commission's unaltered standard contractual clauses (see section 8.2.1 below) should be subject to their express authorisation. Although this is no longer the case, some still require that they be informed of such a transfer and companies should check the current position being taken by their competent supervisory authority. If the European Commission's standard contractual clauses are altered, there is normally an authorisation requirement for the international data transfer.

6.3 Other registration requirements

Under the BDSG, the automatic processing of personal data which involves special risks for the data subject's rights and liberties is subject to examination prior to the beginning of the processing (so-called 'prior checking'). Such prior checking must be carried out when:

- sensitive data are to be processed; or,
- if the purpose of the processing of personal data is intended to assess the personality of the data subject, including his capabilities, his performance or his conduct, unless: (i) there is a statutory obligation to do so; (ii) the data subject has given his consent; or (iii) the processing is required for the conclusion, performance or termination of a contract or a quasi-contractual fiduciary relationship with the data subject.

If a data protection officer has been appointed (see section 7 below), then the responsibility for prior checking will rest with him, and not the supervisory authority.

6.4 Register

The supervisory authorities keep a register of notified automatic processing, which contains for each processing the same information as is provided in the notification. The register, except for the general description of the technical and organisational security measures, and the information about the persons that are entitled to access, can be inspected by anyone.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

In principle, any private body which processes personal data by automatic means has to appoint in writing a data protection officer within one month of commencing its activities, except where the private body as a rule permanently deploys a maximum of nine employees to process personal data by automatic means. A private body also needs to appoint a data protection officer, where personal data are processed other by than automatic means and as a rule at least 20 people are permanently deployed for this purpose.

Private bodies that process certain particularly sensitive data and those companies that are subject to the specific registration regime (see section 6.1.2 above) always have to appoint a data protection officer, irrespective of the number of people permanently deployed to process personal data.

Private organisations may also voluntarily appoint a data protection officer. Where a company has appointed a data protection officer, it is exempt from the notification requirement (see section 5.1.2 above). Data protection officers are therefore quite common. The data protection officer may be a person within the company or an external person.

Data protection officers have certain confidentiality obligations. In order to ensure the independence of the data protection officer, the BDSG lays down requirements as to his abilities, his position within the private body and the obligation of the private body to support him in the performance of his duties, including the provision of resources (assistants, offices, equipment, etc). In particular, the data protection officer must be knowledgeable and reliable. The data protection officer reports directly to the manager and is independent in the exercise of his special knowledge. He may not be prejudiced because of performing his tasks and receives some special protection against the termination of his employment relationship (this was also recently confirmed by a judgment of the German Federal Labour Court (BAG) of March 2011). In November 2010, the German supervisory authorities issued guidance on the minimum requirements that data protection officers must satisfy in their view in terms of know-how, expertise and independence.

Data protection officers have been given an express right to continuing education at the expense of the data controller. In addition, the data controller has certain information obligations *vis-à-vis* the data protection officer. In particular, he must inform the data protection officer of the automatic processing of personal data and provide him with an overview of the information which is ordinarily required in notifications (see section

6.1.5 above), as well as a list of the persons who are authorised to access the respective personal data. The data protection officer has to make this information, except for the description of the organisational and technical security measures taken and the list of the persons that are authorised to access, available to any person upon request. The data protection officer should also be informed in good time of projects for the automatic processing of personal data.

7.2 Tasks and powers

The data protection officer's main task is to work towards ensuring that the data controller complies with the data protection law. For this purpose, he shall monitor the proper use of data processing programmes and take suitable steps to familiarise the persons employed in the processing of personal data with the provisions of and requirements under data protection law. The data protection officer is also responsible for conducting the prior checking (see section 6.3 above). In case of doubt, he may consult the competent supervisory authority. Data subjects may address the data protection officer at any time.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Transfers of personal data to other EU or EEA states are treated like transfers within Germany.

Personal data shall not be transferred to countries outside the EEA, if the data subject has a legitimate interest in the data not being transferred, especially if the bodies abroad fail to ensure an adequate level of protection. The adequacy of the level of protection afforded shall be assessed in the light of all the circumstances surrounding a (set of) data transfer operation(s). Particular consideration shall be given to the nature of the data; the purpose and duration of the proposed processing; the country of origin and country of final destination; the rules of law, both general and sectoral, applicable to the recipient; and the professional rules and security measures applicable to the recipient. Any such data transfers must also comply with all other relevant provisions, in particular the legitimacy and data quality requirements as well as the information obligations and the rights of data subjects.

The European Commission has officially recognised the following countries as providing an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey and Switzerland,.

The body transferring the data shall be responsible for ensuring the lawfulness of the transfer and must inform the body to which the data are transferred of the purpose for which the data are being transferred.

8.2 Legal basis for international data transfers

Personal data may be transferred to bodies, even if no adequate level of protection is ensured, if:

- the data subject has given his consent;

- the transfer is necessary for the performance of a contract between the data subject and the data controller or the taking of pre-contractual steps upon the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract which has been, or is to be concluded, in the interest of the data subject between the data controller and a third party;
- the transfer is necessary to safeguard an important public interest or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from certain public registers.

The transferring party must inform the data recipient that he may only process and use the personal data for those purpose(s) for which the data have been transferred.

It is quite common for companies, especially in the context of customer or consumer personal data transfers, to rely on one of the aforementioned statutory derogations from the prohibition to transfer personal data to third countries. With respect to employees' personal data, the use of the statutory derogations proves to be more difficult as the supervisory authorities have set rather high hurdles. More information in this respect can be found in a working paper issued by the supervisory authorities on international data transfers within a group of companies.

In addition to the above, the competent supervisory authority can authorise individual or a set of transfers by individual decision, provided the data controller adduces adequate safeguards which provide sufficient guarantees as to the protection of the right to privacy and related rights. Such safeguards may in particular be provided by means of contractual measures or so-called binding corporate rules.

8.2.1 Data transfer agreements

The use of data transfer agreements that are based on the European Commission's standard contractual clauses is quite common in Germany. On the other hand, data transfer agreements that are not based on the European Commission's standard contractual clauses are not in use, as for such agreements an authorisation request must be sent to the supervisory authority. An authorisation normally also needs to be obtained where the European Commission's standard contractual clauses have been altered.

Some supervisory authorities require that they be informed where an international data transfer is based on the European Commission's (unaltered) standard contractual clauses and companies should check the current position being taken by their competent supervisory authority.

8.2.2 Binding corporate rules

Adequate safeguards for data transfers may also be ensured by adopting binding corporate rules (BCRs). Seven *Länder* supervisory authorities and the BfDI consider that it is necessary to request an authorisation for data transfers made under BCRs, whereas nine *Länder* supervisory authorities

do not consider an authorisation to be compulsory, although eight would grant an authorisation if the data controller were to apply for it. Germany participates in the so-called mutual recognition procedure. Therefore, if a lead authority in another country has accepted the BCRs, the competent supervisory authority in Germany will usually recognise it.

The use of BCRs is not very common in Germany. Deutsche Post DHL was the first German company to obtain approval for its BCRs under the mutual recognition procedure where a German authority (here the BfDI) acted as the lead authority. The BCR process took four years for DHL, although future processes are said to last only about three months if all relevant documents are provided. It is expected that the use of BCRs will become more popular in the future.

If an authorisation request is sent to the competent supervisory authority, it may be based on the Article 29 Working Party's standard application (WP 133). The German supervisory authorities will closely follow the checklist of requirements laid down in the Article 29 Working Party's Opinion WP 153.

8.2.3 Safe Harbour

The USA is a country which has not been officially recognised as providing an adequate level of protection. However, certain organisations within the USA can sign up to the Safe Harbour scheme, self-certifying that they abide by data protection principles similar to those contained in the Directive. The US Safe Harbour scheme has been recognised by the European Commission as providing an adequate level of protection.

In April 2010, the German supervisory authorities issued a resolution requiring German data exporters to check whether US data importers that have self-certified under the Safe Harbour scheme actually respect the Safe Harbour principles. In particular, they requested that data exporters, as a minimum, check to see when the data importer's Safe Harbour certification was made, verify that (and how) the data importer complies with the obligation to provide notice of the data processing to the relevant individuals, document the assessment and be able to provide evidence when requested by a supervisory authority.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The BDSG imposes a statutory confidentiality obligation on employed persons in data processing which survives the termination of employment. In particular, they may not collect, process or use personal data in an unauthorised manner. In so far as they work for private bodies, on taking up their duties, such persons shall be required to give a written undertaking to maintain such confidentiality. The supervisory authorities have published templates for such undertakings on their websites. The confidentiality obligation also applies to data processors.

9.2 Security requirements

The BDSG obliges data controllers and data processors to take technical and

organisational measures that are necessary to ensure compliance with the BDSG. The technical and organisational security measures are only necessary if the effort is proportionate to the intended purpose of protection.

The BDSG lists the security measures which must be taken in an Annex to its section 9 which includes the following measures (the examples provided for the eight measures below are not contained in the Annex):

- Physical access control: these are measures to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used (eg, securing entries and exits).
- Control of use: these are measures to secure data processing systems from being used without authorisation (eg, locking drives).
- Data access control: these are measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage (eg, screen saver protection).
- Transmission control: these are measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during transport, and that it is possible to check and establish to whom the personal data will be transmitted (eg, regular controls of mobile data carriers).
- Input control: these are measures to ensure that it is possible to subsequently check and establish whether and by whom personal data have been input, modified or removed from data processing systems (eg, logs and audit trails).
- Processor control: these are measures to ensure that, in the case of commissioned processing of personal data, the personal data are processed strictly in accordance with the instructions of the data controller.
- Availability control: these are measures to ensure that personal data are protected from accidental destruction or loss (eg, anti-virus programmes; burglar-, fire- and water-proof server rooms).
- Separation control: these are measures to ensure that personal data collected for different purposes can be processed separately (eg, separate storage).

Encryption is mentioned as an example of the measures for the control of use, data access control and transmission control. The supervisory authorities as well as the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) (BSI) have published numerous guidelines, which provide useful guidance on individual security measures.

9.3 Data security breach notification obligation

A data controller must notify the competent supervisory authority and the data subjects concerned in case certain particularly sensitive categories of personal data have been disclosed illegally or have otherwise come to the knowledge of unauthorised third parties. The notification obligation is limited to the breach of sensitive data, personal data that are subject to

professional or official confidentiality obligations (such as medical secrets), personal data related to (suspected) criminal and administrative offences as well as bank or credit card information.

Notification is only required if as a result of the incident there is a threat of significant harm to the rights and legitimate interests of the affected data subjects. The notification must be made immediately; however, not before appropriate measures for securing the personal data have been taken. Moreover, the notification may also be delayed in case of criminal investigations. In cases where individual notification would require a disproportionate effort, for instance, because of the number of affected data subjects, individual notification is replaced by public notification, which must be made via at least a half-page announcement in at least two daily national newspapers or by other means that would be equally effective.

9.4 Data protection impact assessments and audits

There is no legal obligation for data controllers to carry out data protection impact assessments or audits. Rather, this is left to data controllers' own initiative (for instance, in order to comply with the data minimisation principle (see section 3.4 above)). The BDSG makes reference to the possibility of voluntary audits but leaves the details to be regulated by a separate law. At the end of 2008, the German government adopted a draft act on data protection audits as part of its reform package. However, the draft act on data protection audits failed to clear the legislative process and it is not clear if and when, or in which form it may be revived.

Under the BDSG, data controllers have to check that a data processor has technical and organisational security measures in place prior to commencing the data processing and to carry out further checks regularly thereafter. The results of these checks must be documented. This may require an on-the-spot check of data processors in certain cases, while in other cases data controllers may be able to rely on external audits.

Manufacturers or vendors of IT products can apply for a privacy seal, which is awarded by the supervisory authority of the Land Schleswig-Holstein. This seal certifies the compatibility and compliance of a product with the regulations regarding data protection and data security and requires an evaluation both in technical and legal terms. This procedure, which is rather costly, is not very common. However, this process may become more popular in the future, as the European Commission wants to explore the possible creation of EU certification schemes (eg, privacy seals) for 'privacy-compliant' processes, technologies, products and services.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The supervisory authorities may impose administrative fines. They may also order measures to remedy violations found regarding the collection, processing or use of personal data, or technical or organisational defects. In the case of serious violations or problems, they may prohibit the collection, processing or use, or the use of particular procedures if the violations or

problems are not remedied within a reasonable time despite orders and despite the imposition of the fine.

10.2 Sanctions

The BDSG provides for criminal sanctions and administrative fines in certain cases of a breach of its provisions.

The BDSG creates two types of administrative offences. Type (1) offences may be subject to fines of up to EUR 50,000 and type (2) offences may be subject to fines of up to EUR 300,000. The fines should exceed the economic advantage which the offender received from the administrative offence and for this purpose the aforementioned amounts can be exceeded.

Type (1) offences include:

- failure to notify or incomplete or incorrect or late notification;
- failure to appoint, to duly appoint or to appoint in due time, a data protection officer;
- failure to instruct a data processor correctly, completely or in the required manner or failure to verify compliance with the technical and organisational security measures taken by the data processor before the data processing begins;
- failure to inform the data subject, to inform him correctly or in time;
- in certain cases of the disclosure or use of personal data for other purposes;
- failure to provide the data subject access in full, proper access or access in time and certain other violations of the data subjects' rights; or
- violation of an enforceable order by the supervisory authority.

Type (2) offences include:

- unlawful processing of personal data that are not generally accessible;
- unlawful obtaining of personal data or unlawfully providing access to such personal data;
- obtaining by wrongful statement the transmission of personal data that are not generally accessible; or
- failure to notify a data security breach or incorrect, incomplete or late notification.

Type (2) administrative offences constitute a criminal offence, if they are wilfully committed in exchange for payment or with the intention of enriching oneself or another person or of harming another person. The maximum sentence is imprisonment for up to two years or a fine. Such criminal offences will be prosecuted by the competent authorities only if a complaint is filed by the data subject, the data controller or the competent supervisory authority.

10.3 Examples of recent enforcement of data protection rules

In recent years supervisory authorities have imposed significant fines. For instance, in 2008, a fine of EUR 1.46 million was imposed on German supermarket chain Lidl for several breaches of the German data protection law, including for having instructed several investigative agencies to systematically monitor employees regarding their private life, financial

situation and behaviour, keeping and reading reports of the investigative agencies and for not appointing data protection officers.

In 2009, Germany's rail network, Deutsche Bahn AG, was investigated in relation to several incidents where employees were illegally screened in an effort to combat corruption, but without specific suspicions related to individual employees. Deutsche Bahn AG was also found to have monitored the email communications of all employees who used external email accounts at work. In the end, the CEO of Deutsche Bahn AG was forced to resign and officials faced criminal charges. Deutsche Bahn AG received a fine of EUR 1.1 million for several breaches of German data protection rules, including illegal screening of employees' personal data.

In November 2010, the Hamburger Sparkasse, which is a financial institution, received a fine of EUR 200,000 for having granted external agents access to the account information of Hamburger Sparkasse's clients, without obtaining their consent.

10.4 Judicial remedies

Data subjects may enforce their rights against data controllers before the civil courts under the general civil or commercial law, including by means of injunctive relief and injunctions, or before the specialised courts, in particular labour courts. In addition, they may have a claim against the supervisory authority to take action if this is required to protect the legitimate interests of the data subject and the authority's scope of discretion is reduced.

10.5 Class actions

Class actions are not permitted under German law in the field of data protection.

10.6 Liability

A data subject may claim compensation if a data controller has caused harm to the data subject by the inadmissible or incorrect collection, processing or use of his personal data, unless the data controller acted diligently.

In recent years, court rulings regarding social networking sites have made headlines in the press. For instance, in one case a school teacher filed a lawsuit for an alleged breach of her data protection rights against a website on which pupils could grade their teachers. The lawsuit was dismissed as the court considered the ratings to fall under the fundamental right of freedom of expression.

In January 2009, an ex-employee of a call centre, who had illegally sold a CD containing personal data, including four million bank account details, was condemned by a court to pay a fine of EUR 900.

In November 2010, the former Chief Information Officer of Deutsche Telekom was condemned to imprisonment for three and a half years for a violation of, among others, the telecommunications secrecy rules. In 2005 and 2006 Deutsche Telekom had spied on board members, journalists and trade unionists in order to identify the source of a data leak. For this

purpose, telephone connection data, including telephone numbers, dates and call lengths, were illegally analysed. Deutsche Telekom negotiated with the victims about compensation payments and also voluntarily donated EUR 1.7 million to associations active in the field of data protection.

Hungary

VJT & Partners Law Firm
János Tamás Varga & Zoltán Tarján

1. LEGISLATION

1.1 Name/title of the law

On 11 July 2011, the Hungarian Parliament adopted a new act on data protection, the Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information (New DPA), which will come into effect on 1 January 2012 and will replace Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (DPA). The New DPA aims to guarantee the right of individuals to exercise control over their privacy and to have access to data of public interest and public data on the grounds of public interest. The New DPA implements the Data Protection Directive 95/46/EC (Directive) and is regarded as background legislation for specific statutes regulating the collection and processing of personal data.

In addition to the New DPA, the following statutes are particularly relevant for data protection purposes:

- Act XLVII of 1997 on Processing and Protection of Medical and Other Related Personal Data (Medical Data Act). This regulates the conditions and purposes of the processing of sensitive data concerning an individual's state of health and related personal data;
- Act LXVI of 1992 on Personal Data and Address Records of Citizens. This provides detailed rules on the use of records containing individuals' personal data including their address;
- Act XC of 2005 on Freedom of Information by Electronic Means. This aims to ensure continuous and free-of-charge electronic access to the defined scope of data of public interest, without identification and data request procedures;
- Act C of 2003 on Electronic Communications (Electronic Communications Act). This regulates the processing of subscribers' personal data by communications service providers, including the obligation to retain data;
- Act CXIX of 1995 on Processing of Name and Address Data for Research and Direct Marketing Purposes (Postal Direct Marketing Act). This contains regulations on the processing of name and address data for the purposes of research and paper-based direct marketing;
- Act XXII of 1992 on the Labour Code (Labour Code). This regulates employers' processing of employees' personal data;
- Act LX of 2003 on Insurance Companies and Insurance Activity (Insurance Act). This provides detailed rules on the processing of clients'

personal data that qualifies as an insurance secret;
- Act CXII of 1996 on Credit Institutions and Financial Undertakings (Credit Institutions Act). This regulates the processing of clients' personal data that qualifies as a bank secret;
- Act XLVIII of 2008 on the Basic Conditions of and Certain Restrictions on Business Advertising Activity (Advertising Act). This regulates the processing of personal data for direct marketing purposes;
- Act CVIII of 2001 on Electronic Commercial Services and Services related to the Information Society (Electronic Commerce Act). This provides rules on sending unsolicited electronic commercial communications.

1.2 Pending legislation

See question 1.1.

1.3 Scope of the law

1.3.1 The main players

The main players under the New DPA are the 'data controller', 'technical data processor', 'data subject' and 'third parties'.

The New DPA defines a 'data controller' as any individual or legal person or any organisation without legal personality that:
- determines the purpose of the processing of personal data (alone or together with others);
- makes decisions on data processing (including concerning the means of processing); and
- implements these decisions or has them implemented by a technical data processor.

A 'technical data processor' is any individual or legal person or organisation without legal personality who on the basis of the contract concluded with the data controller – including conclusion of a contract on the basis of legislation – performs technical processing of personal data.

The main distinguishing feature is that the data controller determines the purpose of data processing and makes decisions on data processing. The technical data processor, however, can only perform technical tasks related to data processing operations, and to technically process personal data on the basis of the data controller's instructions. The technical data processor is not entitled to make any decision on the merits concerning data processing.

Under the New DPA the 'data subject' is any specified individual who is identified or can be – directly or indirectly – identified by any personal data.

The New DPA defines the 'third party' as any individual or legal person or any organisation without legal personality that is not identical with the data subject, the data controller or the technical data processor.

1.3.2 Types of data

The New DPA defines 'personal data' as any data relating to a data subject, as well as any conclusion in relation to the data subject, which can be inferred from those data. During data processing, data remain personal data, provided their relation to the data subject can be restored (ie, if the data

controller has those technical means that are necessary for the restoration). Personal data are especially:

- data subject's name;
- identification code;
- one or more pieces of information specific to the data subject's physical, physiological, mental, economic, cultural or social identity.

In practice, personal data are interpreted broadly. As a result, the term 'personal data' covers (among others):

- biometric information;
- sound recordings;
- email addresses;
- IP addresses identifying a computer;
- websites.

In addition to personal data, the New DPA defines sensitive data as: (i) personal data concerning racial origin; national or ethnic minority origin; political opinion or party affiliation; religious or other ideological belief; membership in an interest group; or sexual life; or (ii) personal data concerning health, pathological addiction or criminal personal data.

'Criminal personal data' are any personal data generated during a criminal procedure or prior to that, in relation to crimes or criminal procedures by bodies entitled to carry out the criminal procedure, or to detect crimes, and at penal institutions, which can be associated with the data subject and personal data concerning criminal record.

In addition the New DPA defines the following specific categories of data: data of public interest and public data on grounds of public interest.

'Data of public interest' mean any information – not qualifying as personal data – that is processed by a person or organisation pursuing state, municipal or other public activities and relates to its activity or generated in connection with the public activity.

'Public data on grounds of public interest' mean any data – not qualifying as data of public interest – the publication, availability or accessibility of which is ordered by statute on grounds of public interest.

1.3.3 Types of acts/operations

The New DPA regulates 'data processing', which covers any operation or set of operations performed on data, irrespective of the applied procedure, such as:

- collection;
- obtaining;
- recording;
- organisation;
- storage;
- modification;
- use;
- query;
- transfer;
- disclosure;

- reconciliation;
- combination;
- blocking;
- deletion;
- destruction;
- prevention of their further use;
- photographing, sound or image recording; and
- recording of physical characteristics suitable for the identification of an individual (such as fingerprints and palm prints, DNA samples and iris images).

Contrary to the Directive, the New DPA defines the term 'technical data processing' as the performance of technical tasks related to data processing operations, regardless of the methods or means applied or of the place of application, provided that the technical tasks are performed on the data.

The distinction between data processing and technical data processing can be made on the basis of the definitions of data controller and technical data processor (see section 1.3.1 above).

The New DPA shall also apply to wholly or partially automatic and manual data processing and technical data processing.

1.3.4 Exceptions

The New DPA does not apply to data processing serving solely the own personal purposes of an individual.

1.3.5 Geographical scope of application

The New DPA applies to all data processing and technical data processing performed in the territory of Hungary that either relates to the data of individuals, or to data of public interest or public data on grounds of public interest.

The New DPA applies if a data controller performing data processing outside the territory of the EU:

- entrusts (for the purpose of technical data processing) a technical data processor having its headquarters, premises or residence in the territory of Hungary; or
- uses equipment that is located in the territory of Hungary, except when the equipment is solely used for the transit of data through the territory of the EU.

These data controllers must appoint a representative in the territory of Hungary.

According to the commentary on the DPA, the rules of the DPA also apply to technical data processing contracts, if the data controller based in the territory of Hungary entrusts a technical data processor based outside the territory of Hungary with technical data processing. As the relevant provisions of the New DPA are unchanged compared to the DPA, most probably the above will be applicable in the case of the New DPA as well.

1.4 Particularities

Not applicable.

2. DATA PROTECTION AUTHORITY

National Data Protection and Freedom of Information Authority (the Authority) (*Nemzeti Adatvédelmi és Információszabadság Hatóság*)

At the time of writing, information regarding the address, telephone or fax number or email address of the Authority is not available and its official website has not been set up yet (however, a temporary information website can be found at *www.naih.hu*).

2.1 Role and tasks

In general, the Authority's role is to supervise and facilitate the enforcement of the right to protection of personal data, and to provide access to data of public interest and to public data on the grounds of public interest.

Among others under the New DPA the Authority:

- conducts investigations on request;
- can conduct data protection or 'secret supervisory' administrative procedures on its own initiative;
- can take a case to court in the event of violation of law concerning data of public interest and public data on grounds of public interest;
- keeps the data protection record;
- issues recommendations on a general basis or on request from a data controller;
- can carry out data protection audits on request from a data controller;
- can make recommendations regarding the adoption, modification of laws concerning the processing of personal data and access to data of public interest or public data on grounds of public interest;
- discloses a yearly report on its own activity until 31 March each year and files it with the parliament;
- represents Hungary in the data protection supervisory organisations of the EU.

2.2 Powers

During its investigation the Authority is entitled to inspect all relevant documents, request copies, request information from the data controller or any organisation or person connected with the given case, and enter any premises where data are processed.

In case of violation of law concerning processing of personal data or access to data of public interest and public data on grounds of public interest or imminent danger of it, the Authority calls upon the data controller to remedy the violation of law, or to terminate the imminent danger.

If the data controller fails to comply with the Authority's order relating to processing of personal data, the Authority can launch data protection administrative procedures (however, data protection administrative procedures can be launched without prior investigation if the violation of law requires immediate intervention). In the course of a data protection administrative procedure the Authority can:

- order the rectification of incorrect personal data;
- order blocking, erasure or destruction of personal data processed unlawfully;
- prohibit the unlawful processing or technical processing of personal data;
- prohibit the transfer of personal data to foreign countries;
- order that the data subject must be informed, if the data controller denied the information unlawfully;
- impose a fine (HUF 100,000 – HUF 10,000,000; approximately €370-€37,000); and
- can inform the public of its resolution and the identity of the data controller.

If the data controller fails to comply with the Authority's order concerning the violation of law regarding data of public interest or public data on grounds of public interest, the Authority can take the case to court.

The Authority draws up a report on the investigation if neither an administrative procedure nor a court procedure needs to be launched.

In the case of the probability of unlawful classification of national classified data, the Authority is entitled to launch a 'secret supervisory' administrative procedure.

'National classified data' are any data falling within the public interest that can be protected by classification. If during classification it is established that the disclosure, unlawful acquisition, modification, use, making available to an unauthorised person, or making inaccessible to an authorised person of these data within the specified term of validity directly violates or jeopardises any of the public interests that can be protected by classification, the above administrative procedure may be issued.

If the Authority suspects commitment of a crime, the Authority is entitled to initiate a criminal procedure aimed at the authorised body.

Under the DPA, the Office of the Data Protection Commissioner (the Commissioner) has similar powers, but the Commissioner cannot impose a fine for violation of data protection law.

2.3 Priorities

Information regarding the Authority's priorities for 2012 is not available yet.

The priorities of the Commissioner for 2010/2011 were the following:

- issues of protection of privacy in the press;
- use of surveillance cameras;
- use of the data processed by the public sector for multiple purposes;
- monitoring of the credit reference system; and
- methodology of data protection audit.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Under the New DPA the data subject's 'consent' shall mean any freely given, specific and informed indication of the data subject's will by which he

provides unambiguous approval to the processing of his personal data.

3.1.2 Form

The New DPA requires that the data subject's consent must be:

- given in advance;
- freely given;
- specific; and
- informed.

With regard to 'informed' see section 4.2 below.

Generally, online consent is deemed sufficient, provided it is obtained in compliance with these requirements.

Under the New DPA, consent to data processing must be in writing in relation to sensitive data. However, the data controller bears the burden of proof in relation to the lawfulness of data processing. Therefore, it is always advisable to record a data subject's consent in a retrievable format.

Sector-specific regulation can set out stringent conditions concerning the form of consent. For example, the Credit Institutions Act requires the authorisation for the transfer of personal data qualifying as bank secrets to be contained in a public deed or in a private document of full probative value, or to be provided in writing within the framework of the conclusion of the contract with the financial institution.

Under the New DPA, minors above the age of 16 can give their consent to the processing of their personal data without the consent or the subsequent approval of their statutory representative.

In respect of minors below the age of 16, the rules of Act IV of 1959 on the Civil Code (Civil Code) must be considered regarding the form of their consent. The consent of the minor's statutory representative must be obtained to the processing of the minor's personal data if the minor is under 14. Minors between the age of 14 and 16 can give their consent to the processing of their personal data, however, the statutory representative's approval must be obtained.

Consent from the data subject is deemed to be given:

- in a court procedure or administrative procedure initiated by the data subject with respect to personal data necessary for conducting the procedure;
- in another procedure initiated by the data subject with respect to personal data provided by the data subject;
- with respect to personal data provided by the data subject during his public appearance.

3.1.3 In an employment relationship

The Labour Code provides that the employer can disclose any factual data, or opinion regarding the employee to a third person if it is ordered by statute or the employee consented to it. Neither the New DPA nor the Labour Code requires the fulfilment of additional conditions with respect to the validity of consent. In practice, consent does not qualify as freely given if, for example, the employee may suffer adverse consequences for refusing

to consent.

3.2 Other legal grounds for data processing

With lack of appropriate consent, personal data can be processed if a statute or a local government decree orders the data processing for purposes based on public interest.

Compared with the DPA, the New DPA establishes new legal bases for data processing.

Personal data can be processed if obtaining the consent of the data subject is impossible or it would incur disproportionate cost and the processing of personal data: (i) is necessary for the purpose of performing the legal obligation of the data controller; or (ii) is necessary for the purpose of the legitimate interest of the data controller or a third party and the interest is proportional to the limitation of the right to the protection of personal data.

If the data subject is not able to give his consent due to incapability or for another unavoidable reason, then his personal data can be processed to the extent necessary to protect his or another person's vital interest, or to prevent or avert imminent danger threatening a person's life, safety or possessions during the existence of obstacles to the consent.

If the personal data were obtained on the basis of the data subject's consent, the data controller – unless statute provides otherwise – can process the data obtained: (i) for the purpose of performing his legal obligation; or (ii) for the purpose of the legitimate interest of the data controller or a third party if the interest is proportional to the limitation of the right to the protection of personal data, without any further consent and even after the withdrawal of the consent by the data subject.

With lack of appropriate written consent from the data subject, sensitive data can be processed if:

- it is necessary for the enforcement of an international treaty, or ordered by statute for the purpose of enforcing fundamental rights ensured by the Hungarian constitution, or for the purpose of national security, preventing or combating crimes or national defence (in case of sensitive data specified in point 1.3.2 (i) above);
- ordered by statute for a purpose based on public interest (in case of sensitive data specified in point 1.3.2 (ii) above).

3.3 Direct marketing and cookies

Unless a statute provides otherwise, commercial communications can be sent to an individual via direct marketing, especially via electronic mail or equivalent communications only if the individual has given his prior, unambiguous and explicit consent, except for commercial communications sent via post provided that it is sent at least to 500 addressees (Advertising Act). The consent shall include the name and – if the advertisement for which consent is requested may be communicated only to persons of a certain age – the place and date of birth of the individual; the scope of personal data to be processed; and that the consent was given voluntarily based on appropriate information. The consent can be withdrawn without

restriction and reasoning, free of charge, at any time. The addressee of the commercial communications has to be unambiguously informed of the email and postal address via which he can withdraw his consent to receive such commercial communications. The request for consent must not contain commercial communications.

Sending a request for consent electronically qualifies as sending electronic commercial communications, thus in practice consent cannot be obtained electronically since it must be obtained before any electronic communication is sent (Electronic Commerce Act).

Records of the personal data of individuals who have given their consent to receive commercial communications shall be kept by companies sending commercial communications.

For commercial communications sent via post, the Postal Direct Marketing Act is also applicable.

In accordance with 2009/136/EC Directive implemented by the Electronic Communications Act storing data or gaining access to data stored on the electronic communications terminal equipment of the subscriber or user is only allowed on the condition that the subscriber or user has given his consent, having been provided with clear and comprehensive information, including information on the purpose of the data processing (Electronic Communications Act).

Generally the storage of cookies or equivalent devices on the data subject's terminal equipment is subject to the consent of the data subject.

3.4 Data quality requirements

During data processing the accuracy, integrity and – if it is necessary considering the purpose of data processing – up-to-date nature of personal data have to be ensured, as well as that the data subject can only be identified for the time necessary for the purpose of data processing.

3.5 Outsourcing

Technical data processors:

- cannot make any decisions on the merits of data processing;
- can only technically process the personal data as instructed by the data controller;
- cannot technically process personal data for their own purpose; and
- must store and keep personal data according to the data controller's instructions.

The data controller is responsible for the lawfulness of the instructions given for data processing operations.

In performing his tasks, the technical data processor cannot involve other technical data processors.

In addition, companies interested in business activities using the personal data to be technically processed cannot be entrusted with technical data processing. The interpretation of this provision of the New DPA is not entirely clear. According to legal commentary on the DPA, any company which directly uses the personal data in question for its own profit-making

purposes cannot be entrusted with the technical processing of personal data.

Contracts on technical data processing must be in writing.

3.6 Email, internet and video monitoring

3.6.1 General rules

Emails, email addresses, IP addresses identifying a computer and websites all qualify as personal data, thus monitoring email and internet use qualifies as data processing. The image recording of an individual qualifies as personal data, thus recording the image of individuals by surveillance cameras qualifies as data processing.

The New DPA does not set out special provisions regarding the monitoring of email and internet use and video monitoring, thus the legal bases for monitoring email and internet use, as well as recording of individuals by surveillance cameras are those applicable to data processing in general (see sections 3.1 and 3.2 above).

According to the practice developed under the DPA, operating surveillance camera systems in commonly used areas, for example, in blocks of flats, is subject to the consent of the affected data subjects and requires visibly placed notification. According to Act CXXXIII of 2005 on Person and Property Protection and Private Investigation Activity, persons pursuing property protection activity are entitled to operate surveillance cameras under specific rules. Accordingly, notification regarding the operation of cameras must be placed visibly. Consent can be given by implied conduct, eg consent is deemed to be given if the individual enters the monitored area while aware of the notification.

3.6.2 Employment relationship

According to the practice developed under the DPA, an employer can monitor the email and internet use of an employee under the following conditions:

- the employer supplied the email address and internet use for the purpose of performing work;
- the employer forbade private use;
- the employer notified the employee of the monitoring; and
- the employee gave his consent.

According to the practice developed under the DPA, surveillance cameras cannot be operated for the purpose of monitoring an employee's work or behaviour in places where work is being carried out permanently. Surveillance cameras cannot be operated for any purpose in areas designated for the purpose of spending breaks, or in dressing rooms, toilets and showers.

As an exception to the above rule, surveillance cameras can be operated where the life or safety of employees may be in danger, provided that data subjects have been notified and consent from the data subjects has been obtained.

Similarly, surveillance cameras can be operated for the purpose of protecting assets and valuables stored at the workplace, provided that the data subjects have been notified of their operation in a visible way and

consents from the data subjects have been obtained.

In exceptionally justified cases (eg, at cash desks), when the interest of a data subject clearly requires so, cameras can be operated provided that the data subject consented to it.

4. INFORMATION OBLIGATIONS

4.1 Who

The data controller must provide the data subject with unambiguous and detailed information on all facts relating to the processing of his personal data.

4.2 What

To obtain the data subject's informed consent, the data controller must provide the data subject with unambiguous and detailed information on all facts relating to the processing of personal data, particularly:

- the purposes and legal basis of the data processing;
- persons authorised to carry out the data processing and the technical data processing;
- duration of the data processing;
- the person(s) authorised to have access to the data;
- rights and remedies of the data subject in connection with the data processing;
- personal data that are processed under section 6(5) of the New DPA ie under the following legal basis: if the personal data were obtained on the basis of the data subject's consent, the data controller – unless statute provides otherwise – can process the data obtained: (i) for the purpose of performing his legal obligation; or (ii) for the purpose of the legitimate interest of the data controller or a third party if the interest is proportional to the limitation of the right to the protection of personal data, without any further consent and even after the withdrawal of the consent by the data subject, if applicable;
- whether data processing is based on the consent of the data subject or whether it is mandatory.

4.3 Exceptions

The New DPA does not regulate any exceptions to the main rule.

4.4 When

Unambiguous and detailed information on all facts relating to the processing of the data subject's personal data must be provided prior to the commencement of the processing of his personal data.

4.5 How

The New DPA does not require that the information must be provided in writing but the data controller bears the burden of proof in relation to the lawfulness of data processing, therefore it is always advisable to provide the information in a retrievable format. The information must be provided in an

easily understandable way.

In the case of mandatory data processing, the information can be provided by referring to the provision of the law containing the information specified in section 4.2 above.

If it is impossible or would incur disproportionate costs to inform the data subjects personally, the information obligation can be performed by making the following information public:

- the fact of data collection;
- data subjects affected;
- the purpose of data collection;
- duration of the data processing;
- persons authorised to carry out data processing;
- rights and remedies of the data subject in connection with the data processing; and
- registration number of data processing (if applicable).

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The data subject can request information on the processing of his personal data. The data controller must inform the data subject, on his request, of the:

- data processed by the data controller or technically processed by the technical data processor;
- sources of data processed or technically processed;
- purpose, legal basis and duration of the data processing;
- name, address and activity of the technical data processor in connection with data processing; and
- recipients of the personal data and of the legal basis for transfer.

5.1.2 Exceptions

The data subject's right to access can be refused if:

- statute restricts the data subject's right to access with a view to:
  - (i) promoting the interests of the state's external and internal security, such as national defence, national security, crime prevention or criminal investigation;
  - (ii) promoting state or local governmental economic or financial interest;
  - (iii) promoting significant economic or financial interest of the European Union;
  - (iv) preventing disciplinary and moral offences, or breaches of labour law or labour safety obligations; and
  - (v) protecting the rights of data subjects or of other people;
- the transmitting data controller informs the recipient data controller of specific processing restrictions in relation to processing of personal data under the framework of police and judicial cooperation in criminal matters.

5.1.3 Deadline

The data controller must provide the information in writing and in an easily comprehensible way within 30 days from receipt of the request.

5.1.4 Charges

The provision of information in relation to the specific scope of data is free of charge once per year. Otherwise, the data subject requesting the information can be charged.

5.2 Rectification

5.2.1 Right

The data subject can request the rectification of inaccurate personal data and if the accurate personal data are available to the data controller, then the data controller rectifies them.

5.2.2 Exceptions

If the data controller refuses to rectify the inaccurate personal data, the data controller must inform the data subject in writing of the factual and legal reasons for the refusal within 30 days from receipt of the request. In the case of refusal the data controller informs the data subject of the remedies available to it.

The data subject's right to rectification can be restricted by statute (see section 5.1.2 above).

5.2.3 Deadline

See section 5.2.2 above.

5.2.4 Charges

Under the New DPA the rectification of inaccurate personal data can be requested free of charge.

5.3 Erasure

5.3.1 Right

Personal data must be deleted if:

- their processing is unlawful;
- requested by the data subject (except for mandatory data processing);
- they are incomplete or inaccurate and cannot be corrected in a lawful way, provided that deletion is not prohibited by statute;
- the purpose of processing has ceased to exist, or the legal time limit for the storage of data has expired (except if the storage device containing the personal data has to be archived by virtue of law);
- ordered by a court or the Authority.

5.3.2 Exceptions

If the data controller refuses to erase personal data, the data controller must inform the data subject in writing of the factual and legal reasons for refusal within 30 days from receipt of the request. In the case of refusal the data controller informs the data subject of the remedies available to it.

The data subject's right to erasure can be restricted by statute (see section 5.1.2 above).

5.3.3 Deadline
See section 5.3.2 above.

5.3.4 Charges
Under the New DPA, the erasure of personal data can be requested free of charge.

5.4 Blocking
5.4.1 Right
Under the New DPA, instead of erasing, the data controller blocks the personal data if the data subject so requests, or where it can be assumed that the erasure would have an adverse effect on the legitimate interests of the data subject.

The blocked personal data can be processed only while the purpose of data processing preventing the erasure exists.

5.4.2 Exceptions
If the data controller refuses to block the personal data, the data controller must inform the data subject in writing of the factual and legal reasons for the refusal within 30 days from receipt of the request. In the case of refusal the data controller informs the data subject of the remedies available to it.

The data subject's right to blocking can be restricted by statute (see section 5.1.2 above).

5.4.3 Deadline
See section 5.4.2 above.

5.4.4 Charges
Under the New DPA blocking of personal data can be requested free of charge.

5.5 Objection
5.5.1 Right
The data subject can object to the processing of his personal data if:

- the processing (transfer) of personal data is necessary solely for performing the legal obligation of the data controller or enforcing the legitimate interest of the data controller, the data recipient or third party, except in the case of mandatory data processing;
- personal data are used or transferred for the purposes of direct marketing, public opinion polling or scientific research;
- the right to object is otherwise provided by statute.

5.5.2 Exceptions
See section 5.5.3 below.

5.5.3 Deadline

The data controller must investigate the objection within 15 days from the receipt of it. If the objection is justified, the data controller must discontinue the processing of personal data and block all personal data processed. If the data subject disagrees with the data controller's decision or the data controller misses the 15-day deadline, the data subject can initiate court proceedings within 30 days from receipt of the decision or the expiry of the deadline.

If the data recipient does not receive the data necessary for the enforcement of his right due to the objection of the data subject, the data recipient can initiate court proceedings within 15 days from the notification.

5.5.4 Charges

Under the New DPA the right to object can be exercised free of charge.

5.6 Automated individual decisions

5.6.1 Right

Decisions using solely automated technical data processing based on the assessment of personal characteristics of the data subject can only be made if:

- the decision was made during the conclusion or performance of a contract, provided that it was initiated by the data subject; or
- it was allowed by a statute describing the measures ensuring the legitimate interest of the data subject.

In the case of decisions made by automated technical data processing, the data subject has to be informed about the method applied upon request and he has to be given the possibility to explain his viewpoint.

5.6.2 Exceptions

The New DPA does not regulate any exceptions.

5.6.3 Deadline

The New DPA does not specify a deadline.

5.6.4 Charges

Under the New DPA the data subject's rights regarding decisions made by automated technical data processing can be exercised free of charge.

5.7 Other rights

5.7.1 Right

In the case of violation of his rights, the data subject can initiate court proceedings against the data controller (see section 10.4 below).

Any individual can initiate an investigation before the Authority if any of the following has occurred:

- his rights have been violated in connection with the processing of his personal data or having access to data of public interest or public data on grounds of public interest; or

- there is an imminent danger of violation of his rights (see sections 2.1 and 2.2 above).

5.7.2 Exceptions
The New DPA does not regulate any exceptions to the above right.

5.7.3 Deadline
As a general rule, court proceedings can be initiated within five years from the violation of the data subject's right (the general limitation period under the Civil Code).

5.7.4 Charges
As a general rule, court proceedings are subject to the payment of stamp duty. An investigation of the Authority can be initiated free of charge.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The data controller has to notify the Authority of the information regarding the data processing, as described in section 6.1.2 below.

6.1.2 What
The data controller must notify the Authority, where applicable, of the:
- purpose of data processing;
- the legal basis of data processing;
- categories of data subjects;
- description of data relating to data subjects;
- source of data;
- duration of data processing;
- type of the transferred data;
- recipient of the transferred data;
- legal basis of the transfer;
- technical data processing method applied;
- name and address of the headquarters of the data controller and the technical data processor, the place of data processing and technical data processing and the activity of the technical data processor;
- name and the contact information of the internal data protection officer.

6.1.3 Exceptions
The New DPA specifies exemptions from the notification obligations, such as data processing:
- involving the data of persons having an employment, membership, kindergarten, student, college or – except for customers of financial organisations, public utilities service providers and electronic communications services providers – customer relationship with the data controller;

- according to the internal rules of church or religious communities;
- involving data relating to the diseases or state of health of persons receiving medical care, for purposes of medical treatment or preservation of health or for social insurance claims;
- involving personal data recorded for the purpose of financial and other social support of the data subject;
- involving data relating to the administrative, prosecution and court proceedings of data subjects affected by these procedures or relating to imprisonment;
- involving data processed for the purpose of official statistics, provided the connection between the data subject and the data cannot be restored;
- containing data belonging to a media content provider, which serve solely its own information activity;
- serving the purpose of scientific research, if the data are not published; and
- relating to archived documents.

6.1.4 When

The data controller has to notify the Authority prior to the commencement of his data processing activities, except for mandatory data processing.

6.1.5 How

The New DPA does not specify the language in which the notification must be made to the Authority. According to the practice of the Commissioner developed under the DPA, the notification must be made in Hungarian (a standard form is available on the website of the Commissioner, however, its use is not mandatory). Most probably the above practice will remain unchanged under the New DPA.

The notification must contain all of the information mentioned in section 6.1.2 above. As a general rule the Authority shall register the data processing within eight days from receipt of the notification provided that the notification contains all of the necessary information. If the Authority fails to register the data processing in time, the data controller can commence the data processing according to the notification.

In specific cases the Authority shall register the data processing within 40 days from receipt of the notification, eg, if a financial institution or an electronic communications services provider processes additional client data or uses new technical data processing technology. In these specific cases the Authority registers the data processing on the condition that requirements of lawful data processing are met by the data controller.

6.1.6 Notification fees

Until 31 December 2011 the registration was free of charge, but from 1 January 2012 under the New DPA, the registration – except the notification of mandatory data processing – will be subjected to a registration fee to be specified in separate legislation.

6.2 Authorisation requirements

The New DPA does not regulate any authorisation requirements.

6.3 Register

Until 31 December 2011 the Commissioner held the register of data controllers and their data processing, while from 1 January 2012 the Authority will hold the register of data controllers and their data processing.

The register is public, until 31 December 2011 it could be accessed free of charge by anybody via the website of the Commissioner. From 1 January 2012 the register will be made available on the website of the Authority.

In respect of the content of the register see section 6.1.2 above.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Within the organisation of the following entities acting either as data controller or technical data processor, an internal data protection officer shall be appointed:

- at bodies processing or technically processing national administrative, employment or criminal data files;
- at financial organisations; and
- at electronic communications and public utility services providers.

The internal data protection officer shall have legal, administrative, IT or an adequate higher education degree.

7.2 Tasks and powers

The tasks of internal data protection officer include:

- participating or assisting in decision-making regarding data processing and in ensuring the rights of data subjects;
- supervising compliance with the New DPA, other statutes regulating data processing, internal data protection regulations and data security requirements;
- drawing up the internal data protection and data security regulation;
- keeping the internal data protection register;
- investigating complaints; and
- organising training regarding data protection.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The New DPA does not set out specific restrictions on the transfer of personal data within the European Economic Area (EEA). Similarly, no specific restrictions are imposed on the transfer of personal data to Switzerland on the basis of a treaty on the legal status of the citizens of Switzerland.

Under the New DPA personal data can be transferred to data controllers or technical data processors pursuing data processing or technical data processing activities outside the EEA (and Switzerland) if:

- the data subject has given his explicit consent; or
- the conditions of data processing specified in section 3.2 above are met and an adequate level of protection of the personal data in the third country is ensured during the processing or technical processing of the transferred data.

An adequate level of protection of personal data is ensured if:

- mandatory legislation of the European Union establishes it. In particular, the European Commission has recognised that certain third countries ensure an adequate level of protection as well as US-based organisations that have signed up to the Safe Harbour scheme.
- the parties use standard contractual clauses, which comply with the standard contractual clauses adopted by the European Commission.
- there is a treaty in force between the third country and Hungary safeguarding the rights and remedies of data subjects as well as the independent supervision of data processing and technical data processing.
- the DPA regulates one of the conditions of international data transfer differently from the new DPA. According to the DPA – where there is lack of explicit consent from the data subject – personal data can be transferred to data controllers or technical data processors based outside the EEA (and Switzerland) only if it is allowed by statute and an adequate level of protection of the personal data in the third country is ensured during the processing or technical processing of the transferred data.

8.2 Legal basis for international data transfers

An adequate level of protection of personal data is not required if: (i) the data subject has given his explicit consent; (ii) personal data are transferred for the purpose of implementing an international legal assistance treaty or a treaty on the avoidance of double taxation.

8.2.1 Data transfer agreements

Standard-form data transfer agreements are not in use in Hungary.

The use of the standard contractual clauses adopted by the European Commission is deemed to ensure an adequate level of protection of personal data (see section 8.1 above).

8.2.2 Binding corporate rules

Neither the New DPA nor its official reasoning regulate or refer to the use of binding corporate rules (BCRs).

According to the Commissioner's practice developed under the DPA, BCRs are deemed to ensure an adequate level of protection. However, BCRs in themselves do not serve as a proper legal basis for the transfer of personal data to third country as additional conditions must be met (see section 8.1 above).

8.2.3 Safe Harbour

Under the New DPA, an adequate level of protection of personal data is deemed to be ensured if personal data are transferred to US-based

organisations that have signed up to the Safe Harbour scheme (see section 8.1 above).

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The technical data processor can technically process the personal data solely on the basis of the instructions of the data controller. The technical data processor must not technically process the personal data for his own purposes.

9.2 Security requirements

The data controller, and within the scope of his activities the technical data processor, are obliged to ensure the security of personal data and to take all technical and organisational measures and establish the procedural rules necessary for compliance with the New DPA and other rules relating to data protection and confidentiality.

The personal data have to be protected especially against unauthorised access; alteration; transfer; disclosure; erasure or destruction; accidental destruction and damage; and against becoming inaccessible due to change in the applied technique.

For the protection of data files processed electronically, it must be ensured by appropriate technical solutions that data stored in the records cannot be directly connected and assigned to the data subject, except where a statute allows it.

In the case of automated technical data processing the data controller and technical data processor have to take further measures to prevent unauthorised data inputs and to ensure the tracking down of data inputs and data transfers.

The data controller and technical data processor shall consider technical developments relating to the application of measures serving the security of personal data. Out of the available data processing solutions, the one which ensures a higher level of protection for personal data must be chosen, except where it would cause disproportionate difficulty for the data controller.

9.3 Data security breach notification obligation

There is no general data security breach notification obligation (other than under the Electronic Communications Act, pursuant to which electronic communications services providers are obliged to make a data security breach notification if there is a breach of the security of subscribers' personal data).

9.4 Data protection impact assessments and audits

9.4.1 Who

From 1 January 2013, data controllers can request a data protection audit from the Authority in return for payment of an administrative service fee.

9.4.2 What

During a data protection audit, the Authority evaluates the data processing operations carried out or planned by the data controller on the basis of professional principles specified and published by the Authority.

The Authority can make recommendations to the data controller regarding the data processing.

9.4.3 When

A data protection audit is conducted upon the request of the data controller.

9.4.4 How

Not specified under the New DPA.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

Where there is a violation of law concerning the processing of personal data or access to data of public interest and public data on grounds of public interest or imminent danger to them, the Authority calls upon the data controller to remedy the violation of law or to terminate the imminent danger.

If the data controller fails to comply with the Authority's order relating to the processing of personal data, the Authority can launch a data protection administrative procedure (also a data protection administrative procedure can be launched without prior investigation if the violation of law requires immediate intervention). During the course of the data protection administrative procedure the Authority can:

- order the rectification of incorrect personal data;
- order blocking, erasure or destruction of personal data processed unlawfully;
- prohibit the unlawful processing or technical processing of personal data;
- prohibit the transfer of personal data to foreign countries;
- order that the data subject must be informed, where the data controller denied the information unlawfully;
- impose a fine; and
- can inform the public of its resolution and the identity of the data controller.

Under the DPA the Commissioner has similar powers, eg, he can order blocking, erasure or destruction of personal data processed unlawfully, prohibit the unlawful processing or technical processing of personal data and prohibit the transfer of personal data to foreign countries.

In 2009 the Commissioner declared that the operation of surveillance cameras in the block of flats – with no consent from all residents – was unlawful, therefore the Commissioner prohibited the further operation of the surveillance cameras and ordered the erasure of the personal data collected.

In 2010 the Commissioner declared that the mayor's office of a Hungarian city disclosed a list of personal data belonging to persons, who claimed

financial support from the city but refused to take it over on its website unlawfully, considering that the mayor's office did not have legal basis to disclose these personal data. As a result, the Commissioner ordered the destruction of the list, the erasure of the list from the website of the city and prohibited the disclosure or transfer (including data transfer to foreign countries) of the personal data.

In 2011 the Commissioner established that personal data of the citizens who participated in the 'Social Consultation 2011' were processed unlawfully. During the 'Social Consultation 2011', a government body acting as data controller sent a questionnaire to all Hungarian citizens having residence in Hungary. To ensure the legal basis of the processing of the personal data of the citizens, the questionnaire included a consent declaration. Having examined the consent declaration, the Commissioner established that it did not meet the requirements set out in the DPA, thus the data processing of the government body was unlawful. As a result, the Commissioner ordered the destruction of personal data collected and prohibited creation of a database from the data obtained during the consultation and also prohibited the related data processing and technical data processing.

10.2 Sanctions

According to Act IV of 1978 on the Criminal Code, 'abuse of personal data' is the act of any person (for unlawful profit making purposes or that causes a significant violation of interest) involving the:

- processing of personal data without legal basis or contrary to the purpose of the data processing; or
- failure to take measures serving the security of the data.

The penalty for this offence is up to one year's imprisonment.

Any person not fulfilling the obligation to provide the data subject with information and as a result, significantly violating the interests of others, is similarly punished. If an individual commits the abuse of personal data in relation to sensitive data, the penalty is up to two years' imprisonment.

If an individual commits abuse of personal data as an official person or by using a public commission, the penalty is up to three years' imprisonment.

In addition, minor offences are punished by a fine for example:

- failure to report, register or provide data required by law;
- providing false data intentionally; and
- hindrance of the supervision of the respective authority.

With regard to administrative sanctions see section 10.1 above.

10.3 Examples of recent enforcement of data protection rules

Not applicable.

10.4 Judicial remedies

The data subject can initiate court proceedings where his rights have been violated or if the data subject disagrees with the data controller's decision regarding his objection (see section 5.5.3 above). If the court rules in favour

of the data subject, the court can oblige the data controller to provide the data subject with the requested information, to rectify, block or delete the data, withdraw the decision made by automated technical data processing, or to consider the data subject's right to object.

The court can make its judgment public if the interests of data protection and the rights protected by law of a greater number of data subjects require it.

In the court procedure, the data controller bears the burden of proof and must prove that data processing complies with the relevant legislation.

10.5 Class actions

Class actions are not used in Hungarian data protection practice and neither the DPA nor the New DPA regulate them.

10.6 Liability

The data controller is liable for damages resulting from unlawful data processing or violation of the data security requirements (with the exception of force majeure and cases when the damage was caused intentionally by the claimant or by the claimant's material negligence).

In practice, court decisions ordering the payment of damages for violation of data protection law are not very common in Hungary. Nonetheless, for example in 2007 the court ordered the defendants to pay the data subject HUF 500,000 (approximately €1,850) as compensation for unlawful disclosure of information concerning the alcohol addiction of the data subject.

India

Desai Desai Carrimjee and Mulla Naheed Carrimjee

1. LEGISLATION

1.1 Name/title of the law

India does not at present have a single statute which deals with data protection and privacy laws.

There are several statutes in force in India which cover data protection and privacy issues both directly and indirectly. The major statutes are listed below:

- The Constitution of India;
- The Information Technology Act 2000 (IT Act);
- The Credit Information Companies (Regulation) Act 2005 (CICRA 2005);
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Information Technology Rules 2011)

1.1.1 Indian Constitution

The Indian Constitution makes no specific mention of privacy, but the nation's courts have found an implicit, but nevertheless basic, right of privacy in the Constitution.

In India, the right of privacy has been derived through judicial decisions, from the rights available under Articles 19(1) (a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution. The Supreme Court has held that even though the right to privacy is not expressly enumerated as a fundamental right, it could certainly be inferred from the fundamental rights guaranteed under the Constitution.

1.1.2 IT Act

The IT Act is often presented, in India, as the text regulating data protection under Indian law. The IT Act contains provisions for the facilitation of electronic commerce and also the filing of e-commerce documents with government agencies. The IT Act was amended by the IT (Amendment) Act 2008 and two new sections, 43-A and 72-A, were inserted dealing with data protection.

Section 43 provides protection against unauthorised access to a computer system by imposing a heavy penalty up to Rupees one crore (approximately €142,857). The unauthorised downloading, extraction and copying of data are also covered under the same penalty. Clause 'c' of this section imposes a penalty for the unauthorised introduction of computer viruses. Clause 'g' provides penalties for assisting unauthorised access.

Section 43-A prescribes compensation in the event that a body corporate which possesses, deals or handles any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and consequently causes wrongful loss or wrongful gain to any person. This section makes no mention of non-digital data.

Section 72-A offers protection against non-consensual breach of confidentiality and privacy, and *inter alia* states that any person including an intermediary who whilst providing services under the terms of a lawful contract, secures confidential information belonging to another person, and with intent to cause wrongful loss or gain, discloses such information to any other person, shall be punished with imprisonment for a term which may extend to three years or with a fine of up to Rupees Five Lacs (approximately €7,142).

CICRA 2005

The CICRA 2005 is a law that regulates 'credit information companies' (credit bureaux), 'credit institutions' (credit providers), and others with access to credit information ('specified users'). This legislation provides a comprehensive data protection code for credit information companies and institutions. The Reserve Bank of India is the regulatory body under the Act.

The CICRA 2005, regulations and rules set up overlapping data protection requirements. Chapter VI of the CICRA 2005 sets out the information privacy principles applying to credit information companies, credit institutions and specified users. The principles require credit information companies, company credit institutions and specified users to adopt certain privacy principles.

The Credit Information Companies Rules, made by the government, include steps and safeguards for privacy protection to be taken by credit institutions and by credit information companies and specified users. These include the institution of an appropriate policy and procedure duly approved by the board of directors, steps for ensuring the accuracy of data prior to publishing them, data security and system integrity safeguards. Further obligations regulating all parties in relation to unauthorised access, use or disclosure and 'fidelity and secrecy' complete the obligations. The Rules provide for an appellate authority for any grievances by the agent of an aggrieved company or the credit information company as the case may be.

The Information Technology Rules 2011

On 7 February 2011, the Department of Information Technology (MCIT) published draft rules on its website (The Information Technology Rules 2011) in exercise of the powers conferred by the IT Act, which were issued in their final form in April 2011.

1.2 Pending legislation

The Personal Data Protection Bill 2006 was introduced in the Upper House of Parliament on 8 December 2006. The purpose of this bill is to provide for

the protection of personal data and information of an individual collected for a particular purpose by one organisation, and to prevent their use by any other organisation for commercial or any other purpose and entitle the individual to claim compensation or damages due to disclosure of personal data or information on any individual without his consent and for matters connected with the bill or incidental to the bill. Provisions contained in this Bill relate to the nature of the data to be obtained for the specific purpose and the quantum of data to be obtained for that purpose. It defines 'personal data' as information or data which relate to a living individual who can be identified from that information or data whether collected by any government or any private organisation or agency.

1.3 Scope of the law

1.3.1 The main players

IT Act

The IT Act was created to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as 'electronic commerce'.

The IT Act aims to facilitate electronic commerce and also to redress abuses of it and provide for the adjudication and settlement of disputes. The IT Act as originally enacted did not provide for sanctions against the abuse of protected data, however this has been amended via the insertion of section 43-A which seeks to provide compensation to persons who suffer damage or loss due to a body corporate's failure to secure its information.

Privacy has always been an area of statutory ambivalence in India. Certain statutes protect the privacy of information whereas other statutes render its protection as absent. India, via the amendment of the IT Act, and the insertion of section 43-A into the IT Act has sought to adopt a similar approach to the protection of privacy as that adopted and prescribed by the European Union.

Section 43-A of the IT Act seeks to protect sensitive personal information which is held by private intermediaries. It attempts to provide this protection by prohibiting the unauthorised disclosure of sensitive personal data or information. The term 'body corporate' is also defined in this section to *inter alia* mean a company and shall include a firm, sole proprietorship, or any other association of individuals engaged in commercial or professional activities. If such a body corporate is negligent in adhering to reasonable security practices or procedures *vis-à-vis* sensitive personal data it shall be liable to pay dues for the wrongful loss or wrongful gain to any person so affected. The definition of 'body corporate' in section 43-A is deemed to include all private associations of persons but it does not include state or government associations or organisations.

Section 43-A has been further amended by the Information Technology Rules 2011. These rules seek to define and make explicit the meaning of 'reasonable security practices and procedures' which is vaguely defined in section 43-A. The Information Technology Rules 2011 *inter alia* list the information security policies which ought to contain managerial, technical,

operational and physical safety measures for the protection of information. The Information Technology Rules 2011 also stipulate a mandatory privacy policy.

CICRA 2005

This Act was passed in order to provide for the regulation of credit information companies and for matters connected to them. It applies to any person who seeks financial assistance from a credit institution and is applicable to credit institutions which include banks, non-banking financial companies, public financial institutions, financial corporations, companies engaged in the business of credit cards and any other institutions which the Reserve Bank of India may specify.

Section 19 specifies that a credit information company in possession of credit information shall take such steps including security safeguards to ensure that the data relating to the credit information maintained by them are accurate and duly protected against any loss or unauthorised access or unauthorised disclosure.

1.3.2 Types of data

IT Act

Pursuant to the IT Act, 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and are intended to be processed, are being processed or have been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

The 2008 amendment to the IT Act refers to 'sensitive personal data' in section 43 but fails to define what exactly it means by sensitive personal data.

Sensitive personal data are defined under the Information Technology Rules 2011 as information relating to a data subject's:

- password;
- financial information, such as bank account, credit card, debit card or other payment instrument details;
- physical, physiological and mental health condition(s);
- sexual orientation;
- medical records and history;
- biometric information;
- any information relating to the above.

Information that is freely available or accessible in the public domain, or furnished under the Right to Information Act 2005 or any other law in force, is not regarded as sensitive personal data.

It is important to note that the IT Act only applies to sensitive personal data. Other types of information have thus far not been protected through the 2008 amendment.

CICRA 2005

'Personal data' are not defined (or used) in the CICRA 2005, but are defined in the Credit Information Companies Regulations 2006 as *'such other data relating to an individual other than…'* the information that credit reporting participants are allowed to collect by the rules made under the Act. This would include identification and location data. It is important to remember that 'personal data' therefore do not include 'credit information'. It is not the more general term, but rather the complement to 'credit information'. 'Data' are defined in the Credit Information Companies Rules 2006 as facts which are collected or furnished to a credit information company which form part of the credit information relating to a borrower or client.

1.3.3 Types of acts/operations

IT Act

Under the IT Act, rules pertaining to data protection include cyber contraventions related to unauthorised access to computers, computer systems, computer networks or resources; and unauthorised alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data or computer databases.

Data in entirely non-automated systems would therefore not be covered by the Act, but data in non-electronic form which had previously been the subject of processing could be.

Section 43-A of the IT Act provides that while processing, dealing and handling any sensitive personal data or information, a body corporate must maintain reasonable security practices and procedure.

The Indian government has introduced, with effect from 13 April 2011, the Information Technology Rules 2011, which regulate the collection, disclosure, transfer and storage of sensitive personal data and widen the scope of the regulation provided in section 43-A .

The disclosure of personal data is regulated by section 72-A of the IT Act, which places an obligation on a person who obtains any material containing personal information while providing services under the terms of a lawful contract (data processor), from disclosing the personal information without the consent of the data subject or in breach of contract.

The restriction on disclosure of personal data provided for in section 72-A of the IT Act which applies to all persons who acquire personal data while rendering services under a lawful contract.

The obligation to maintain reasonable security practices while processing sensitive personal data is limited to a body corporate, defined as any company engaged in commercial or professional activities.

Under the 2011 Rules, the restrictions on collection, disclosure, transfer and storage of sensitive personal data apply to a body corporate and any person acting on its behalf.

CICRA 2005

This Act seeks to regulate the information provided to credit information companies and incidental matters connected to it.

Section 20 of the Act specifies that every credit information company, credit institution and specified user shall adopt the certain privacy principles in relation to the collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information, *inter alia* being the principles which may be followed by every credit institution, specified user, credit information company from its respective member institutions, or any other principles which the Reserve Bank may consider necessary and appropriate and as may be specified by Regulations.

1.3.4 Exceptions

IT Act

Data in entirely non-automated systems are not covered by the Act. All data other than sensitive personal data as defined are not covered. Government institutions are not covered under the IT Act 2000.

CICRA 2005

CICRA 2005 provides, *inter alia*, for the protection of all information relating to the nature of loans or advances, the nature of security, the guarantees furnished, the creditworthiness of any borrower of a credit institution or any other matter as specified by the Reserve Bank of India. It will not cover any information of a like nature which is submitted to an intermediary who is not a credit institution as defined under CICRA 2005.

1.3.5 Geographical scope of application

IT Act 2000

The IT Act applies to the whole of India and to any offence or contravention of it committed outside India by any person. The IT Act also applies to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

The IT Act's extra territorial jurisdiction is prescribed in section 1(2) where it is stated to extend to any offence or contravention committed outside India by any person. The underlying reason for this section is that on the internet the notions of territoriality are undermined.

However the applicability of section 43-A has been restricted to a body corporate located within India only through a press release issued by the Ministry of Communications and Information Technology dated 24 August 2011, relating to the Rules prescribed under section 43-A of the IT (Amendment) Act 2008, which reads *inter alia* as follows: *'Any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5 and 6.'*

CICRA 2005

The provisions of CICRA apply to the whole of India.

1.4 Particularities

India is not a signatory to the APEC Privacy Framework. India has however attempted to emulate the European Union framework for the protection of personal data through the insertion of section 43-A of the IT Act 2000 and the Sensitive Personal Data Rules issued under it.

2. DATA PROTECTION AUTHORITY

India has no dedicated data protection authority. The Indian government has announced from time to time its intention to set up a three-member Data Protection Authority of India (DPAI). Among other things, the DPAI would monitor and enforce compliance with any future proposed data protection laws and investigate any data security breaches.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Under the Information Technology Rules 2011, when processing sensitive data, a body corporate must ensure that the obligations relating to consent by data subjects are followed.

The change to the IT Act that has attracted the most attention is the requirement that a body corporate must get consent from the provider of information for the purpose for which the information is being collected and the means and modes of the use of such information. Consent has not been defined under the rules but it is stated as prior permission under Rule 6 of the Information Technology Rules 2011.

The key issue to note here is that consent must come from the person who provided the information and not compulsorily from the individual to whom the information relates. This makes the rule much less burdensome than might originally be envisaged. For example, where the processing of sensitive personal information is outsourced to a service provider in India, the service provider has only to seek the consent from its customer who is the 'provider of information' *vis-á-vis* the service provider. Whether that customer must, in turn, obtain the consent of the individual to whom the information relates depends on the data protection laws that apply to the customer in the jurisdiction where the information is being collected.

A body corporate is also required to obtain permission from the provider of information before disclosing the information to a third party, except where the disclosure is agreed to in the contract between the body corporate collecting the data and data subject, or necessary for compliance with a legal obligation. Consent is not required where government agencies are mandated by law to obtain sensitive personal data for the following reasons (Rule 6 of the Information Technology 2011 Rules):

- verification of identity;
- prevention, detection or investigation of cyber incidents; or
- prosecution and punishment of offences.

A third party receiving information from a body corporate is obliged to not disclose the information further.

3.1.2 Form
Disclosure of sensitive personal information or data by a body corporate to any third party shall require the prior permission of the person disclosing such information and this permission has to be given by way of a lawful contract. This is provided in Rules 6 and 7 of the Information Technology Rules 2011.

3.1.3 In an employment relationship
Not applicable.

3.2 Other legal grounds for data processing
The Sensitive Personal Data Rules set out specific provisions relating to sensitive personal data. Sensitive personal data are defined in Rule 3. Rule 4 outlines the basis under which personal data are to be collected. Rule 6 states that personal sensitive data shall only be disclosed to a third party with prior permission from the provider of such information, unless such disclosure is required for legal compliance.

3.3 Direct marketing and cookies
Because India does not have a general data protection law, privacy protection against direct marketing is found in relation to specific intrusions such as telemarketing or spam.

3.3.1 Telemarketing internally within India
In October 2007, the Telecom Regulatory Authority of India (TRAI) launched the National Do Not Call (NDNC) database, authorised under the Telecom Unsolicited Commercial Communications Regulations 2007.

3.3.2 Telemarketing overseas from India
The NDNC is intended to protect Indian consumers, not to protect foreigners, who are unable to utilise the NDNC as it requires subscriber numbers to be lodged with telecoms providers.

India has not yet legislated in relation to spam – unsolicited internet commercial communications – or cookies.

3.4 Data quality requirements
Rule 5 of the Information Technology Rules 2011 states that a body corporate shall:

- ensure that it does not retain information for longer than is required for the lawful purposes of the information; and
- ensure that the information is used for the purpose for which it was collected.

Sensitive personal information must also be collected for a lawful purpose connected with a function or activity of the body and the collection of information must be necessary for that purpose.

3.5 Outsourcing

Neither the IT Act nor the CICRA 2005 deal specifically with outsourcing. However, Indian Business Processing and Outsourcing (BPO) companies, in addition to compliance with India data protection laws, also adhere to major US and European regulations in the field of data protection through contractual arrangements.

3.6 Email, internet and video monitoring

3.6.1 General rules

The IT Act 2000 and the Rules framed thereunder are applicable.

Chapter 7, section 35 of the IT Act 2000 provides for the grant of an electronic signature by the certifying authority. Section 43 provides for damages, penalty and compensation for damage to a computer or computer systems due to unauthorised access and computer contaminants. Chapter 10 provides for the establishment of a Cyber Appellate Tribunal. Chapter 11 outlines the offences *inter alia* for tampering with computer source documents, computer-related offences, punishments for sending offensive messages, punishment for identity theft, punishments for violation of privacy, punishment for sexually explicit information in electronic form, and for cyber terrorism. Section 66 outlines the punishment for privacy-related computer offences. The penalties for different offences include imprisonment for up to three years and/or a fine which may extend to One Lakh Rupee (approximately €1,428).

3.6.2 Employment relationship

Not applicable.

4. INFORMATION OBLIGATIONS

In principle, there is no right in India for data subjects to be informed of any matters at the time of collection of personal information, except in relation to credit information. However, under the Information Technology Rules 2011, a body corporate or person processing personal data on its behalf is required to implement a privacy policy for handling and dealing with user information including sensitive personal information.

4.1 Who

Under Rule 4 of the 2011 Rules, a body corporate, while processing, dealing with or handling sensitive personal data, or a person who collects, receives, possesses, stores, deals or handles information on its behalf, must have a privacy policy published on its website. In relation to credit information, the obligation lies with the credit institutions.

4.2 What

Under the Information Technology Rules 2011, the privacy policy must cover the type of personal information being collected and the purpose, means and modes of usage of such information. The privacy policy must state the following:

- clear and easily accessible statements of the body corporate's practices and policies;
- the type of personal or sensitive personal data collected;
- the purpose of collection and use of the information;
- the circumstances in which disclosure of information is made to third parties;
- reasonable security practices and procedures;
- reasonable steps to ensure that the data subject is aware of the fact that the information is being collected; the purpose of the collection; the intended recipients of the information; and the name and address of the agency collecting the information and the agency retaining the information.

In relation to credit reporting, the data subject must be informed of the content of his credit information whenever it is the basis for refusal of credit. Credit reporting participants must take reasonable steps to inform a person, whenever they collect personal data (which excludes credit information), the purposes for which the data are collected.

When a credit institution or other specified user denies credit or any other service on the basis of a credit information report, they must within 30 days provide the person denied in writing with the specific reasons for rejection, a copy of the credit information report, and the name and address of the credit information company concerned.

4.3 Exceptions

Not applicable.

4.4 When

Not applicable.

4.5 How

Under the Information Technology Rules 2011, the privacy policy must be made available to those providing information to the body corporate under a contract. For example, if the personal information is being collected through a website, it is possible to simply include the link to the privacy policy.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The Information Technology Rules 2011 provide that a body corporate shall ensure that the data subject can review the information provided as and when requested.

Public sector information

The Right to Information Act 2005 applies to every 'public authority' established under the Constitution or a central or state law, or a notification or order by a government, and includes any body owned, controlled or substantially financed, or non-government organisation (NGO) substantially

financed, directly or indirectly by government funds.

Subject to exceptions in the Act, all citizens have 'the right to information'. The right does not therefore extend to non-citizens. The 'right to information' applies to any information 'held by or under the control of any public authority', and includes inspections, certified copies, and 'obtaining information … in any other electronic mode or through printouts where such information is stored in a computer'.

Citizens can therefore access their own records under the Act. Where some part of the information they seek to access is exempt under section 8, section 10 requires that as much information as can be severed must be provided.

All information which is in the public domain is exempt from the classification of 'sensitive personal data or information' under the Information Technology (Rules 2011.

5.1.2 Exceptions

The right under the Right to Information Act 2005 does not extend to non-citizens.

5.1.3 Deadline

Not applicable.

5.1.4 Charges

Not applicable.

5.2 Rectification

There is no right to correction of personal information in either the IT Act 2000 or the Right to Information Act 2005. Although under the latter Act the Central Information Commission or State Information Commissions can receive complaints from a person 'who believes that he or she has been given incomplete, misleading or false information under this Act' these references to incompleteness and falsity do not refer to the nature of the personal information about the individual, but instead to a comparison between what is really in the government records and what is disclosed.

5.2.1 Right

The Information Technology Rules 2011 provide that a body corporate shall ensure that any personal or sensitive information (or information found to be inaccurate or deficient) is corrected or amended where feasible.

The CICRA 2005 allows borrowers or clients to ask any credit reporting participant to 'update' the credit information that they hold, 'by making an appropriate correction or addition or otherwise'.

5.2.2 Exceptions

Not applicable.

5.2.3 Deadline

Not applicable for the Information Technology Rules 2011.

Information under CICRA 2005 must be provided within 30 days.

5.2.4 Charges
Not applicable.

5.3 Erasure
Not applicable.

5.4 Blocking
Not applicable.

5.5 Objection
The Information Technology Rules 2011 also provide an option to the data subject not to provide the data sought to be collected, and to withdraw consent under Rule 5.

5.6 Automated individual decisions
Not applicable.

5.7 Other rights
Not applicable.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
Not applicable.

6.2 Authorisation requirements
Not applicable.

6.3 Other registration requirements
Not applicable.

6.4 Register
Not applicable.

7. DATA PROTECTION OFFICER
7.1 Function recognised by law
Not applicable.

8. INTERNATIONAL DATA TRANSFERS
8.1 Applicable rules
Under the IT Act, there is no restriction on the transfer of personal data outside India. However, any transfer of personal data, whether to a group company or otherwise outside India, requires consent from the data subject where the personal data are obtained by the person or entity transferring the data while performing services under a lawful contract.

In addition, sensitive personal data can only be transferred to an entity

outside India that maintains the same level of data protection adhered to by the body corporate transferring the data as provided for under the 2011 Rules. The transfer of sensitive personal data is permitted only in certain circumstances. This is elaborated above in section 3.5.

Export of credit information

The strict restrictions on to whom credit information can be disclosed by Credit Information Companies (CIC) will also apply to disclosures to overseas enquirers, whether credit providers or credit bureaux. These overseas parties would not qualify as a 'specified user' and could therefore not obtain information from a CIC, unless the Reserve Bank made regulations deeming them to be credit institutions.

8.2 Legal basis for international data transfers

8.2.1 Data transfer agreements

There is no approved standard form for data transfer agreements.

A data transfer agreement is sufficient to legitimise a transfer of data provided consent for processing and transfer of data has been obtained at the time of obtaining the data. However, restrictions on transfer of data can apply in certain circumstances. The rules and procedures governing the transfer of data are outlined under the IT Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2009 and the CICRA 2005.

8.2.2 Binding corporate rules

Not applicable.

8.2.3 Safe Harbour

Not applicable.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Not applicable.

9.2 Security requirements

Under the Information Technology Rules 2011, a 'grievance officer' must be designated, who must deal with any grievances from data subjects within one month of the date of their receipt.

The Sensitive Personal Data Rules set out which measures constitute 'reasonable security practices and procedures' for the purposes of section 43-A of the IT Act. A body corporate must implement security practices and procedures which include a comprehensive documented information security programme and information security policies. The information security policies should contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

Organisations following IS/ISO/IEC 27001 codes shall be deemed to

have implemented reasonable security practices and procedures. Industry associations or industry clusters that follow security standards other than IS/ISO/IEC 27001 codes are required to get them approved by the government.

9.3 Data security breach notification obligation

In the event of an information security breach, the body corporate must demonstrate, as and when called on to do so under the law, that it has implemented security control measures under its documented information security programme and information security policies. The body corporate or person on its behalf shall be required to demonstrate when called to do so by an agency mandated by law. This agency has not been notified under the IT Rules 2011. Corporates may also opt to self regulate by following the international standard IS/ISO/IEC 27001. Such corporates who opt for self-regulation shall be deemed to be in compliance under the IT Rules 2011 if they have been certified or audited with respect to them by an independent auditor duly certified by the Central Government. However, there is no specific requirement to notify personal data security breaches to data subjects in the 2011 Rules.

9.4 Data protection impact assessments and audits

Not applicable.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

10.1.1 General

There is no public authority in India which as yet has any significant overall responsibilities for enforcing data protection provisions. Other than the National Human Rights Commission (NHRC), which does not have enforcement powers, there is no organisation to which complaints about interferences with privacy can in general be made for the purposes of initiating an investigation. As noted, the NHRC does not yet play any role in relation to privacy. However, courts of law have jurisdiction to try offences relating to breach of privacy.

10.1.2 Enforcement powers of the national regulator

There is no national regulator to enforce the provisions of the IT Act. However, contraventions of sections 43 and 43-A of the IT Act are adjudicated by an adjudication officer to be appointed by the Government of India. The Secretary of the Ministry of Information Technology in each state is appointed as the adjudicating officer.

10.1.3 Conciliation and arbitration

If 'borrowers and clients' are involved in a dispute concerning the business of credit information for which the CICRA 2005 provides no remedy, 'such disputes shall be settled by conciliation or arbitration as provided by the Arbitration and Conciliation Act 1996'. The Reserve Bank is to appoint the arbitrator.

10.2 Sanctions

Section 66 of the IT Act 2000 provides protection against hacking. Under this section, 'hacking' is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss or damage will be caused to any person and information residing in a computer resource which is either destroyed, deleted, altered or its value and utility diminished. This section imposes the penalty of imprisonment of three years or a fine of up to two Lakhs Rupees (approximately €2,857) or both on the hacker.

Section 72-A of the 2008 amendment to the IT Act prescribes punishment for disclosure of information in breach of a lawful contract. Any person who, in the course of providing services under a lawful contract gains access to any material containing personal information, discloses without consent, or in breach of the contract, this material to anyone else will be punished. This section imposes a penalty of up to five Lakhs Rupees (approximately €7,142) and/or with imprisonment which may extend for up to three years.

Contravention of section 72-A of the IT Act is a penal offence and attracts criminal liability where the disclosure of personal information is made with the intent to cause, or with knowledge that there is a likelihood of causing, wrongful loss or wrongful gain to the person concerned.

The penal liability includes either or both imprisonment for up to three years and/or a fine of up to five Lakhs Rupees (approximately €7,142).

The punishment for any offences committed under the CICRA 2005 include imprisonment and may also include a monetary fine of up to one crore (approximately €142,857).

The CICRA 2005 Chapter VIII provides offences and penalties for wilful breach of the privacy principles for knowingly providing false credit information.

10.3 Examples of recent enforcement of data protection rules

The data protection laws are not presently actively enforced; however, there is a growing awareness of data protection requirements.

10.4 Judicial remedies

Indian courts have jurisdiction to hear cases concerning breaches of the implied constitutional right of privacy. The courts also have jurisdiction to hear cases filed under the IT Act 2000 and CICRA 2005.

10.5 Class actions

In the recent case of *Dr Harsh Pathak v Union of India & Ors*, a public interest suit filed by a lawyer in the Supreme Court regarding unsolicited phone calls, the Supreme Court of India passed an interim order restricting cellular companies from making promotional calls.

10.6 Liability

The breach of obligations imposed by section 43-A of the IT Act 2000 results

in civil liability for the body corporate to compensate the affected person by payment of damages.

The breach of any confidential or proprietary information can also be protected through a contract between two parties. This may be contractually reflected via an agreement between the parties and interpreted according to the provisions of the Indian Contract Act 1872. The Indian courts have upheld the protection of confidential and proprietary information rights this way.

Israel

Yigal Arnon & Co Yoheved Novogroder-Shoshan[1]

1. LEGISLATION

1.1 Name\title of the law

The Protection of Privacy Law 1981 (Privacy Law) is the main Israeli law dealing with the collection and use of personal data. The Privacy Law is supplemented by various regulations, including:

- Protection of Privacy Regulations (Determination of Databases Containing Non-Disclosable Data) 1987;
- Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies) 1986 (Data Possession Regulations);
- Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect) 1981 (Data Inspection Regulations);
- Protection of Privacy Regulations (Fees) 2000;
- Administrative Offences Regulations (Administrative Fine – Protection of Privacy) 2004;
- Protection of Privacy Regulations (Transfer of Information to Databases outside of the State's Boundaries) 2001 (Data Transfer Regulations);
- Protection of Privacy Order (Determination of Public Bodies) 1986;
- Protection of Privacy Order (Determination of the Investigatory Authority) 1998;
- Protection of Privacy Order (Establishment of Regulatory Unit) 1999.

The right to privacy is recognised as a fundamental human right under the quasi-constitutional Basic Law: Human Dignity and Liberty, which provides that: *'every person is entitled to privacy and to the confidentiality of his life' and 'there shall be no infringement of the confidentiality of a person's conversations, correspondence and writings'*.

In addition, certain sector-specific laws provide additional protection for the types of information referenced in such laws. Among these are the Patients' Rights Law 1996 (medical information); Genetic Information Law 2000 (genetic information); the Psychologists' Law 1977 (information disclosed in the context of psychological treatment); the Banking Ordinance 1941 (financial data); and the Credit Information Service Law 2002 (credit information).

Unless otherwise specifically set forth to the contrary below, the responses relate to the Privacy Law as supplemented by complementary regulations and case law.

[1] *The author is grateful to Miriam Friedmann for her assistance in preparing this chapter.*

1.2 Pending legislation

Two major pieces of legislation are pending. The draft Protection of Privacy Law (Authority of Enforcement) 2010 would amend the existing provisions of the Privacy Law to grant the Registrar of Databases (Registrar) additional investigatory, supervisory and enforcement powers, including the power to impose fines that are substantially higher than those currently authorised under the Privacy Law. The intention is to enable the Registrar to exercise certain powers that are currently held only by the criminal enforcement authorities.

The draft Protection of Privacy Regulations (Information Security in Databases) 2010, if enacted, would impose additional obligations in respect of data security (including relating to physical security requirements, access controls, outsourcing, data destruction and maintenance of backup files) and would require the performance of risk assessments under certain circumstances.

1.3 Scope of the law

The Privacy Law establishes guidelines for the protection of privacy in general, as well as guidelines relating to databases. Personal information not held in a database (as defined under the Privacy Law (see section 1.3.2 below)) is not regulated by the Privacy Law's database provisions, but such information may be used only subject to the Privacy Law's general privacy provisions. Many activities involving database information can also result in civil and criminal liability for invasion of privacy.

Section 2 of the Privacy Law lists 11 activities which constitute an infringement of privacy if they are performed without consent. A number of these activities are relevant to data protection, such as:

- copying a letter or electronic message not intended for publication or using its contents without the permission of the sender or the recipient, provided that the letter or electronic message does not have historic value and 15 years have not passed from the date it was written;
- infringing an obligation of secrecy laid down by law in respect of a person's private affairs;
- using, or passing on to another, information on a person's private affairs, other than for the purpose for which it was given;
- publishing or passing on anything that was obtained by way of an infringement of privacy under certain provisions of the Privacy Law;
- infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person's private affairs; and
- publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain.

Section 2 of the Privacy Law also prohibits spying on or trailing a person in a manner likely to harass him, or any other harassment; this prohibition may be relevant in certain contexts in which privacy issues are implicated, such as online behavioural monitoring or use of location data.

This chapter addresses only the regulation of databases.

1.3.1 The main players

The Privacy Law governs the use of database information by any person or entity.

The Privacy Law does not use the term 'data subject', however, the definitions of 'person', 'data' and 'database' indicate that the Privacy Law's database provisions apply only to databases containing information about natural persons. In addition, the rights of inspection and correction of database information (which are discussed more fully below) are accorded solely to natural persons. The Privacy Law does not require that the individual be a resident or citizen of Israel.

It should be noted that while the definition of 'person' for the purposes of determining what constitutes an 'infringement of privacy' indicates that only an individual's privacy is protected by the Privacy Law, case law indicates that notwithstanding the definition in the law, corporations may, to some extent, be entitled to protectable privacy rights under the Privacy Law (Civ Petition 1614/02, in Civ File 2324/01 *Multilock Ltd v Rav Bariach Hashkaot Ltd* Tak-Mehozi 2002 (1) 851) and under the Basic Law (Civ File 10434/96 *Keisarit v Ararat* Tak-Mehozi 2000 (3) 26643). Therefore, although the law in this respect is not settled, it appears that the privacy rights of legal persons, although generally thought not to exist, may be afforded some protection under Israeli law.

The Privacy Law identifies three primary actors in connection with databases:

'Database owner' is not defined in the Privacy Law. A note on the draft Protection of Privacy Regulations (Information Security in Databases) 2010 compares the role of the database owner to that of the European 'data controller', however, the Privacy Law does not state as a general rule that the database owner is primarily responsible for data protection compliance, and allocation of responsibility between database owners and holders is as set forth in the Privacy Law provisions, many of which are described in this chapter.

'Database holder' is defined as a person who has a database in his possession on a permanent basis and is permitted to use it.

'Database manager' is defined as the active manager of the legal entity which owns or possesses a database, or a person authorised to carry on such activities by the manager for this purpose.

1.3.2 Types of data

'Data' are defined as details regarding a person's personality; personal status; private affairs; state of health; economic situation; professional qualifications; opinions; and faith. The Supreme Court has indicated a willingness to interpret the term 'data' broadly, and the term 'private affairs' is often construed by Israeli courts as encompassing various types of personal information that are not specifically mentioned in the definition above. For example, Supreme Court decisions have held that individuals' addresses, telephone numbers, bank account information national ID numbers, and IP addresses constitute data.

'Sensitive data' are defined as details regarding a person's personality, private affairs, state of health, economic situation, opinions and faith (ie, information included within the definition of 'data' other than personal

status and professional qualifications). In addition, 'sensitive data' include other information deemed to be sensitive data by order of the Minister of Justice with approval from the Constitution, Law and Justice Committee of the Knesset (no such order has been issued to date).

The Data Possession Regulations create an additional category of information called 'restricted data', which includes data about a person's health; data subject to the provisions of sections 13(e) of the Privacy Law (ie, primarily databases related to security, defence foreign affairs, law enforcement, taxation, and money laundering); and any other data deemed 'restricted' by an order of the Minister of Justice (no such order has been issued to date).

'Database' is defined as '*a collection of data, stored by magnetic or optical means and intended for computer processing*', other than the following two specific kinds of databases: (i) any collection of data for personal use that are not used for business purposes; and (ii) a collection of data that contains only names, addresses and means of communicating with the data subject (eg, telephone, email address or fax numbers) which in itself does not create any characterisation that infringes the privacy of the people whose names are included in it, so long as neither the owner of the collection nor any body corporate under the owner's control has an additional collection of data (albeit unrelated to the first collection).

Collections of data that cannot be manipulated in a computerised manner (for example, collections of paper records, but not scanned versions of such records) are not included within the definition of 'database.' For this reason Directive 95/46/EC of the European Parliament, pursuant to which the European Commission formally adopted a decision recognising that Israel's domestic law guarantees an adequate level of protection for personal information for the purposes of Article 25 of the EU Data Protection Directive 95/46/EC applies only to international automated data transfers, as well as non-automated transfers that are subject to further automated processing in Israel, but not to international data transfers where the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means.

1.3.3 Types of acts/operations

The Privacy Law expressly addresses the following activities in respect of databases:

- managing a database;
- holding a database;
- using a database.

'Use' is defined as including, but not being limited to disclosure, transfer and delivery. While the Privacy Law does not specifically address or define the 'processing' of data, it can be presumed that processing activities are included within the definition of 'use'.

1.3.4 Exceptions

As described above, the following collections of data are not considered 'databases' under the Privacy Law: (i) collections of data that cannot be

manipulated in a computerised manner (ie, collections composed exclusively of paper records not in digital form); (ii) any collection of data for personal use that is not used for business purposes; and (iii) a collection of data that contains only names, addresses and means of communicating with the data subject (eg telephone, email address or fax numbers) which in itself does not create any characterisation that infringes the privacy of the people whose names are included in it, so long as neither the owner of the collection nor any body corporate under the owner's control has an additional collection of data. In addition, collections of data that do not relate to a 'person' as defined in the Privacy Law are not considered 'databases' under the Privacy Law and are not subject to the law's database provisions.

1.3.5 Geographical scope of application

Generally, the jurisdictional application of Israeli laws is limited to acts within Israel, although exceptions to this rule can be carved out in primary legislation or by case law. However, if the restrictions on the transfer of data (see section 8 below) are breached, any subsequent use of the data outside Israel is likely to be attributed to the party in Israel who breached the transfer restrictions.

1.4 Particularities

It should be noted that in January 2011, pursuant to the EU Data Protection Directive 95/46/EC, the European Commission formally adopted a decision that Israel's domestic law guarantees an adequate level of protection for personal information for the purposes of Article 25 of Directive 95/46/EC. This places Israel within the select number of jurisdictions so recognised by the European Commission. The decision applies to international automated data transfers, as well as non-automated transfers that are subject to further automated processing in Israel, but not international data transfers where the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means.

2. DATA PROTECTION AUTHORITY

In 2006, the Israeli Law Information and Technology Authority (ILITA) was established. ILITA sits within the Israeli Ministry of Justice, its head serves as the Registrar, and the ILITA staff implements the Registrar's functions. Technically, ILITA is comprised of the three statutory law and technology regulators set up under the Privacy Law, the Electronic Signature Act 2001 and the Credit Reporting Act 2002. Within ILITA, there are departments responsible for legal matters, enforcement and investigation, and registration and supervision. ILITA represents Israel in the international privacy arena and participates in the legislative process. Prior to the formation of ILITA, the Registrar served as Israel's data protection authority.

2.1 Role and tasks

The Registrar supervises the registration of databases, maintains the Registry of Databases, and supervises compliance with the Privacy Law and the regulations issued under it.

2.2 Powers

The Registrar is responsible for the registration and supervision of databases and is also the head of a unit set up by the Minister of Justice to supervise databases, their registration and the security of database information. The Registrar is authorised to appoint inspectors who are granted broad powers under the Privacy Law, including the right to demand that a person furnish information and documents related to a database. To ensure implementation of the Privacy Law and to prevent breaches, an inspector may enter any place in which he has a reasonable suspicion that a database is being operated, and search and seize any item (including computer equipment and output) if he is persuaded that doing so is necessary for the enforcement of the Privacy Law.

2.3 Priorities

The Registrar increasingly makes use of its supervisory and investigatory powers, including by performing investigations of businesses suspected of not complying with Privacy Law obligations. It is presumed that many of these efforts are aimed at preserving the confidence of EU countries following Israel's recognition by the European Commission as having an adequate level of protection for personal information. Indeed, many of the guidelines issued recently by the Registrar refer to terms and principles that appear in European legislation but do not appear in the Privacy Law (for example, certain of these guidelines call for data breach notifications and risk assessments, though these are not expressly required under the Privacy Law).

3. LEGAL BASIS FOR DATA PROCESSING

The Privacy Law does not expressly address the processing of personal data. However, as mentioned above, 'use' is defined as including, but not limited to, disclosure, transfer and delivery, and it can be presumed that processing activities are included within the definition of 'use'.

3.1 Consent

Consent is not necessarily required for the processing of personal data in a database so long as the information is used for the purpose for which it was provided. However, where data are collated without the consent of the data subject, the resulting database must be registered.

3.1.1 Definition

'Consent' is defined under the Privacy Law as informed consent, express or implied. While Israeli courts have not yet defined what constitutes informed consent for the purposes of the Privacy Law, in other contexts courts have interpreted 'informed consent' as consent granted after provision of information to an individual, which would be understood by a reasonable person, that is reasonably necessary for the purposes of providing consent.

3.1.2 Form

Consent may be express or implied. In many contexts, such as employment and health, it is standard practice to obtain written consents for the use,

processing and transfer of personal information.

3.1.3 In an employment relationship

Courts scrutinise consent very closely in employment contexts so that any suggestion, or even the subjective suspicion, of detrimental changes to the employee's conditions of employment can be deemed to be duress and so undermine the consent. In addition, any information gathered must be used for legal purposes, essential interests or a legitimate purpose and meet the proportionality test. As a matter of good practice, employment agreements governed by Israeli law should include the employee's express consent to the collation of personal data, including sensitive data, to the transfer of such data outside Israel and to the use of data for human resources management purposes.

3.2 Other legal grounds for data processing

In most situations, data processing will involve use of a database (as defined under the Privacy Law), and thus the notice requirement applicable to solicitations of information for inclusion in a database will apply (see section 4 below). There is no provision similar to Article 7 of the EU Data Protection Directive, but data must only be used and processed for the purpose for which they were provided.

3.3 Direct marketing and cookies

The Privacy Law regulates the operation and holding of databases used for direct mail services. 'Direct mail' is defined as *'an individual approach to persons, based on their belonging to a population group, as determined by one or more characteristics of those persons whose names are included in the database'*. An 'approach' includes one made in writing or in print, whether made via telephone, facsimile, computer or other means. 'Direct mail services' are defined as *'the provision of direct mail services to others by way of transferring lists, adhesive labels or data by any means whatsoever'*.

The Privacy Law prohibits a person from managing or possessing a database that is used for direct mail services unless it is registered and one of its stated purposes is direct mail services. A person who manages or possesses a database used for direct mail services must keep a record stating the source of the data, the date the data were received and the persons to whom the data were given.

Approaches by direct mail must state clearly: (i) that it is a direct mail solicitation; (ii) the registration number of the database; (iii) that the recipient of the solicitation has the right to be deleted from the database and the address to be contacted for this purpose; (iv) the identity and address of the database containing the data from which the solicitation was made; and (v) the sources from which the owner of the database received that data.

Every person has the right to demand that the owner of a database used for direct mail delete from the database any information relating to him or that personal information not be given to a specific person, to a category of persons, or to any person at all, whether for a specific or indefinite period of

time. The owner of the database must comply with these requests and give written notice of the fact that he has complied. If such notice is not given to the person within 30 days after the owner receives the request, then the person may apply to the Magistrates' Court for an order that the owner of the database comply with the request.

In December 2008, Israel enacted Amendment No. 40 to the Israeli Communications Law (Bezeq and Broadcasting) (Communications Amendment). The Communications Amendment prohibits the distribution of 'promotional messages' (defined below) by email, fax, automated calling system or electronic messages (SMS) without the recipient's opt-in (ie, obtaining the recipient's prior express consent), and its provisions are in addition to the Privacy Law provisions applicable to direct mail activities. The Communications Amendment defines 'promotional messages' as any commercial message which encourages the purchase of a product, service or other expenditure. The Communications Amendment applies equally to entities offering the goods or services themselves, and entities distributing electronic advertisements on their behalf. Consent may be obtained in writing, by electronic message or recorded conversation. Advertisers may contact business recipients once in order to solicit such consent; such initial contact will not be considered a violation of the Communications Amendment. Recipients may revoke their consent at any time, either in writing or in the same medium used to transmit the advertisement. It is permitted to distribute promotional messages without prior consent of the recipient under limited circumstances.

In addition to the consent requirements described above, the Communications Amendment requires that all electronic promotional messages include a clear, conspicuous notice containing the following information:

- identification of the promotional message as an advertisement. For email communications, the word 'advertisement' must appear in the email subject line; in all other promotional messages, such identification must appear in the beginning of the promotional message;
- the advertiser's identity and contact information; and
- notification of the recipient's right to opt out of receiving promotional messages and means for opting out (including an email address for email advertisements).

Israel does not have specific legislation directed to the use of cookies. Thus, the general privacy and data protection principles discussed elsewhere in this chapter will apply to the collection of information using cookies and use of such information.

3.4 Data quality requirements

Owners, holders and managers of databases are each responsible for data security, and 'data security' is defined to include, *inter alia*, the 'integrity of data' – ie, that the information in the database is identical *'to the source from which it was derived, without having been changed, delivered or destroyed without due permission'*. See also question 9.2 below.

3.5 Outsourcing

Outsourcing activities generally implicate the Privacy Law provisions applicable to databases, 'database holders' (since service providers will often qualify as database holders) and cross-border transfers of database information.

In 2011, ILITA published Directive 2-2011 for outsourcing activities. Under the directive (the legal status of which is not clear but which indicates the Registrar's interpretation of applicable law):

- service providers should preferably be given access to databases maintained and controlled by the database owner rather than receiving copies of databases;
- there should be an intercompany agreement expressly designating the scope and term of permitted access to and use of databases, ensuring the service provider's compliance with applicable laws (including notification requirements by the data subject, his rights to examine and correct the data, the need to separate different databases from different sources) and deletion of information following termination of the service period (unless keeping a copy is required by law or for the purposes of protection from lawsuit);
- it is recommended that a data security officer be appointed at both the client and service provider's facilities;
- entities outsourcing activities should create a binding data security policy; and
- the party outsourcing work should perform periodic service provider audits (and, when appropriate, surprise audits) to ensure compliance with obligations, and implementation of procedures for the service provider's transmission of breach notifications.

The guidelines do not limit other obligations existing under law.

3.6 Email, internet and video monitoring

3.6.1 General rules

Monitoring activities are highly regulated in the employment arena (see discussion below). Other monitoring activities will be subject to the general principles set forth in the Privacy Law and case law, including, without limitation, the prohibitions on violating personal privacy without consent and provisions applicable to databases (including, without limitation, the requirement that information in registered databases be used only for the purposes for which the database was registered, as well as the notice requirements for solicitations of database information (see section 4 below)).

With respect to email monitoring, copying or use of the content of an electronic message or other written communications not intended for publication without permission of the sender or intended recipient constitutes a breach of privacy unless the communication is of historic value or 15 years have passed since the day of writing; therefore, most email monitoring activities will require data subjects' consent.

In 2010 ILITA issued an opinion addressing video monitoring in public places. While the opinion primarily addresses video monitoring by public authorities, due to the practical difficulties involved in obtaining data

subject consent to video monitoring, the opinion and its recommendations are also directed at private entities performing monitoring activities in public places (under Israeli law, 'public places' are not limited to areas owned or managed by public authorities). While the opinion does not have the status of binding law, it demonstrates what the Registrar views as appropriate measures to be taken in relation to video monitoring.

Pursuant to the opinion, the following requirements are prerequisites to video monitoring activities in public places:

- performance of a privacy impact assessment addressing the specific purpose of video monitoring, the matters described below and evaluation of whether viable, less invasive alternatives exist;
- identification of a specific legitimate purpose for video monitoring, and results of monitoring may not be used beyond the specific legitimate purpose;
- video monitoring must meet the proportionality test, whereby it can be demonstrated that video monitoring is the most efficient and appropriate means for achieving the desired purpose, that such purpose cannot be achieved by less invasive means, and that the benefits will exceed the attendant invasion of privacy rights;
- the video monitoring must be implemented in a manner that causes least invasion of privacy (where cameras are situated, times during which they are activated, resolution, etc); and
- the public must be notified of video monitoring activities (for example, using appropriate signage).

If the results of video monitoring are maintained in database form, the database laws and regulations will apply. If the video monitoring will have voice recording capabilities, other requirements (such as the Eavesdropping Law 1979) will apply.

3.6.2 Employment relationship

Israel's highest labour court recently issued a decision which establishes for the first time comprehensive rules regarding employers' monitoring of employees' computer, information technology and email use at the their workplace. This decision stipulates that monitoring personal email correspondence requires a court order or employee consent in each instance; thus, in the wake of this decision, on a practical level it is difficult for employers to monitor employee communications unless the company IT policy prohibits employees' use of email for non-business purposes.

Pursuant to the labour court ruling the following are prerequisites for monitoring employees' computer, information technology and email use:

- Legitimate purpose. Monitoring must be in the interest of a legitimate business purpose. Data collected by virtue of monitoring activities may not be used in a manner different from the pre-defined legitimate purpose. The employer must examine alternative surveillance technologies which involve the lowest degree of violation of employee privacy.
- IT policy. The employer must implement a policy regarding computer

usage at the workplace and surveillance activities. This policy must be incorporated in the employment agreement.

- Detailed notice. The IT policy must provide specific and detailed notice regarding monitoring activities to be undertaken which includes: express notice that email communications will be monitored and for what purpose; description of monitoring and surveillance measures and technologies which will be used (identifying specific programs); identification of frequency of monitoring activities and which communications will be monitored; the manner in which the gathered data will be kept and stored; the duration of such storage; and what use, if any, will be made of the stored data. To the extent the employer intends to employ blocking technologies (for example, blocking transmission of emails containing certain types of data or access to certain websites) the employer must clearly detail the scope of such technologies and their use.
- Written consent. The employee must consent in writing to the violation of his privacy (certain mandatory language is required to appear in the consent) and this consent must be part of the employment contract. The consent must be explicit, informed and voluntary, after the employee has been notified of the employer's intention to violate the employee's privacy interests.
- Third party notice. Third parties must be notified of surveillance activities (for example, by means of an email footer containing appropriate disclosure).

As this decision was only recently enacted, the requirements for implementing certain of these requirements remain somewhat unclear and have not yet been clarified by subsequent court decisions. Many Israeli companies are currently engaged in efforts to comply with the ruling.

4. INFORMATION OBLIGATIONS

Any solicitation of information for inclusion in a database or use as part of a database must be accompanied by a notice to the data subject.

4.1 Who

Any person or entity soliciting information for inclusion in a database.

4.2 What

The notice must indicate: (i) whether the person has a legal obligation to deliver the requested data or whether delivery is voluntary; (ii) the purpose for which the data are requested; and (iii) to whom data will be delivered and for what purpose.

4.3 Exceptions

The notice requirement applies to information included in a database. Thus it does not apply to solicitations of data to be stored in a form that will not constitute a 'database' as defined under the Privacy Law.

4.4 How

No specific form of notice is required.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The Privacy Law provides that an individual may inspect any information about the individual that is kept in a database, whether in person, by a representative who has written authorisation, or by a guardian (eg in the case of minors). The owner of the database must enable inspection of the information in Hebrew, Arabic or English, as requested. Where a database is maintained by a third party (ie, the database holder), the database owner must refer the applicant to the holder and provide the holder's address. Also, the database owner must give written instructions to the holder to permit the inspection. If the applicant applied first to the database holder, then the holder must inform the applicant whether he holds information about the applicant and provide the database owner's name and address.

The Data Inspection Regulations permit (but do not require) the database owner to provide a print-out of the requested information in lieu of permitting inspection of the data within the database. The person viewing the print-out may not remove the print-out from the premises of the database owner or holder without permission.

5.1.2 Exceptions

The right of access does not apply where:

- the data concern the applicant's physical or mental health and the database owner believes that the data may endanger the applicant's life or cause severe harm to the applicant's physical or mental health (in such cases, the database owner must deliver the data to a physician or psychologist on behalf of the applicant); or
- the data are privileged (for example, information held by attorneys, physicians, psychologists, or social workers) and access constitutes a violation of the privilege pursuant to statutory or judicial law, unless the applicant is the person for whose benefit the privilege is enacted.

In addition, the right of inspection does not apply to the following databases and data:

- a database of a security authority (ie, the police, the intelligence branch of the General Staff , the military police of the Israel Defence Forces, the General Security Service, the Institute of Intelligence and Special Assignments, and the Witness Protection Authority);
- the prison service database;
- a tax authority's database;
- data to which the security of the state, its foreign relations or the provisions of any enactment require that they not be disclosed;
- databases of any body deemed (by the Minister of Justice, in consultation with the Minister of Foreign Affairs or Defence, with approval of the Parliament Foreign Relations and Security Committee) to contain information that should not be revealed due to national security or foreign relations ('secret information'). Databases deemed to contain secret information include the databases of the Ministry

of Defence and certain of its affiliates, and the Israel Aircraft Industry and its subsidiaries and operating units. However, any person who asks to inspect data about himself stored in such a database is entitled to examine any information that is not 'secret information';
- databases of investigations and law enforcement, including those maintained by the Police Investigation Department in the Ministry of Justice (in matters of investigations and enforcement), the Israel Securities Authority (in matters of investigations), and the Israel Antitrust Authority (in matters of investigations); and
- the database established by the Minister of Justice in accordance with section 28 of the Prohibition of Money Laundering Law 2000, which contains a record of all reports of money laundering submitted to the Ministry of Justice. This database is governed by the Prohibition on Money Laundering Regulations (Guidelines for Management of the Database and the Protection of Data contained in it), 2002.

A database holder may refuse the request for inspection if the database is held by a 'service bureau' that processes and stores data for its customers, so long as the applicant is referred to the owner of the data on whose behalf the processing or storage services are performed. If the owner of the database refuses to permit inspection, the applicant must be notified within 21 days (which may be extended by the Registrar for 15 additional days).

5.1.3 Deadline

Inspection must be permitted within 30 days of the data subject's request, although the Registrar may extend the period by an additional 15 days.

5.1.4 Charges

The owner or holder of the database is entitled to impose a fee of NIS 20 for the inspection.

5.2 Rectification

5.2.1 Right

If an individual's inspection reveals that database information is inaccurate, incomplete, unclear or not up to date, the individual may request that the database owner (or, if the owner is a foreign resident, the database holder) amend or delete the information. If the database owner agrees to the request, he must make the necessary changes and communicate them to the applicant and to anyone who received the information from him within the preceding three years.

5.2.2 Exceptions

No exceptions are foreseen.

5.2.3 Deadline

If the database owner refuses the request for correction, then he must give the person notice of the refusal within 30 days of receipt of the request (which may be extended for an additional 15 days by the Registrar). The holder of the database must correct the data if the database owner agreed to

the requested amendment, or if a court ordered the correction to be made.

5.2.4 Charges
The issue of charging is not addressed.

5.3 Erasure
5.3.1 Right
There are no provisions in the Privacy Law or regulations regarding erasure of data in databases generally. However, a person may demand in writing that the owner of a database used for direct mail delete the information about him from the database. In addition, recent non-binding communications originating from the Registrar derived from the Privacy Law provide an obligation to remove database information when its intended purpose has expired.

5.3.2 Exceptions
Not applicable.

5.3.3 Deadline
Not applicable.

5.3.4 Charges
Not applicable.

5.4 Blocking
5.4.1 Right
The Privacy Law and regulations do not include provisions regarding blocking of data in databases generally. However, every person may demand in writing from the owner of a database used for direct mail, or from the owner of a database containing data on the basis of which the direct mail approach was made, that data relating to him not be given to a specific person, to a category of persons, or to any person at all, either for a specific or indefinite period of time.

5.4.2 Exceptions
Not applicable.

5.4.3 Deadline
Not applicable.

5.4.4 Charges
Not applicable.

5.5 Objection
Since the Privacy Law does not specifically address processing of data, the law does not create a general right to object to such processing. However, the Privacy Law allows a data subject to object to processing of data by means of a civil suit based on the claim that the processing is an infringement of privacy or constitutes an act or omission in violation of Chapters Two or

Four of the Privacy Law. A limited right of objection exists with respect to direct mail services (see section 3.3 above).

5.5.1 Right
Not applicable.

5.5.2 Exceptions
Not applicable.

5.5.3 Deadline
Not applicable.

5.5.4 Charges
Not applicable.

5.6 Automated individual decisions
5.6.1 Right
The Privacy Law does not create any such right.

5.6.2 Exceptions
Not applicable.

5.6.3 Deadline
Not applicable.

5.6.4 Charges
Not applicable.

5.7 Other rights
Not applicable.

5.7.1 Right
Not applicable.

5.7.2 Exceptions
Not applicable.

5.7.3 Deadline
Not applicable.

5.7.4 Charges
Not applicable.

6. REGISTRATION OBLIGATIONS
Database owners are required to register certain databases with the Database Registrar.

The Privacy Law and regulations do not impose obligations to notify the

Registrar of data processing operations or data transfers.

6.1 Notification requirements

6.1.1 Who

Database registration requirements apply to the database owner. However, the Privacy Law prohibits managing or holding a database that is required to be registered but has not been registered; thus database managers or database holders could also face liability in connection with a database that is not registered in the manner required under law.

6.1.2 What

The owner of a database must register the database if any of the following conditions is met:

- the database contains data about more than 10,000 people;
- the database contains sensitive data;
- the database contains data about natural persons not provided by them, on their behalf or with their consent;
- the database belongs to a public body (as defined under section 23 of the Privacy Law; or
- the database is used for direct mail.

In addition, the Registrar has the power to order that databases which are exempt from the obligation to register pursuant to the exception above must nonetheless be registered. The Registrar has not yet used this power.

6.1.3 Exceptions

Even where one of the conditions above are met, the database registration requirements do not apply where the database only contains information made public by lawful authority, or which was made available for public inspection by a lawful authority. This exemption recognises that under Israeli law, certain databases must be open to public inspection, such as the database containing information about companies pursuant to the Companies Law 1999. The Registrar has the power to order that databases that are exempt from the obligation to register pursuant to the exception above must nonetheless be registered. The Registrar has not yet used this power.

6.1.4 When

A database must be registered prior to managing or holding the database, unless the Registrar permits performing such acts prior to registration.

6.1.5 How

Applications to register a database must be submitted to the Registrar using the application form published by the Registrar and available (in Hebrew) on the ILITA website, *www.justice.gov.il/NR/rdonlyres/1E830B68-FC40-4B60-A154-45BA9C144863/12412/tofesrishummaagar.pdf*. The application must specify the following:

- the identity and address in Israel of the owner of the database, the database holder and the manager of the database;

- the purpose for setting up the database and the purposes for which the information is intended;
- the types of data to be included in the database;
- details regarding transfers of data outside the borders of the state; and
- details regarding any regular receipt of data from a public body, the name of the public body providing the data and the nature of the data, with the exception of details delivered by the public body with the consent of the data subjects.

In addition, the general manager of the database owner must notify the Registrar in writing of the name of the database manager for inclusion in the Registry.

The owner or holder of a database must notify the Registrar if there is a change in the details provided in the application, or if operation of the database is discontinued. If the Registrar deems it appropriate with respect to the actual operations of the database, the Registrar is authorised to register a purpose different from that specified in the application, to register a number of purposes for a database, or to order that several applications be submitted instead of the single application that was submitted.

Following submission of the application for registration of a database, the Registrar must register it in the register within 90 days, unless the Registrar has reasonable grounds to assume that the database is used or is liable to be used for illegal activities or as a cover for illegal activities or the data included in the database were obtained, accrued or collected in violation of the Privacy Law or in violation of the provisions of any other legislative enactment. If the Registrar does not register the database within 90 days and does not inform the applicant that registration has been refused or delayed, then the applicant is permitted to manage or hold the database even if it is not registered. However, if the Registrar does inform the applicant of a refusal or delay in registration, then the applicant may not manage or hold the database unless a court decides otherwise.

6.1.6 Notification fees

Pursuant to the Privacy Regulations (Fees) 2000, as amended in December 2010 and January 2011, the initial fee for database registration is NIS 251. An additional annual fee is imposed on registered databases for subsequent calendar years, with the exception of databases owned by the State of Israel. The amount of the fee is determined taking into account the owner of the database and its contents. The fee for the registration of a database owned by a corporation, other than a non-profit organisation, is NIS 939 if the database contains sensitive data concerning more than 10,000 people; NIS 501 for sensitive data concerning 10,000 people or less; and NIS 251 for any other database. Registered databases not owned by a corporation, or owned by a non-profit organisation, are exempt from payment, unless the database contains sensitive data concerning more than 500 people, in which case the fee is NIS 250. Special discounts are granted to owners of multiple databases.

6.2 Authorisation requirements

Not applicable.

6.2.1 Who
Not applicable.

6.2.2 What
Not applicable.

6.2.3 Exceptions
Not applicable.

6.2.4 When
Not applicable.

6.2.5 How
Not applicable.

6.2.6 Authorisation fees
Not applicable.

6.3 Other registration requirements
6.3.1 Who
Not applicable.

6.3.2 What
Not applicable.

6.3.3 Exceptions
Not applicable.

6.3.4 When
Not applicable.

6.3.5 How
Not applicable.

6.3.6 Registration fees
Not applicable.

6.4 Register
The Registrar is required to maintain a Registry of Databases. All of the details required to be included in the application for registration must be included in the Registry. The Registry is open for public inspection (with the exception of certain governmental databases such as the police and those maintained by the military and tax authorities).

7. DATA PROTECTION OFFICER
7.1 Function recognised by law
The following entities must appoint a suitably trained person to be in charge

of data security ('the Security Officer'):
- entities holding five or more databases requiring registration;
- public bodies, as defined in section 23 of the Privacy Law; and
- banks, insurance companies or companies involved in ranking or evaluating credit.

The database manager must inform the Registrar as to the identity of the Security Officer.

7.2 Tasks and powers

While the Security Officer is to be responsible for data security, the database owner, holder and manager nevertheless are each held individually responsible under the Privacy Law for data security as well.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Under the Data Transfer Regulations, the transfer of data from databases within Israel to a location outside the State of Israel is strictly prohibited unless the database owner secures the written undertaking of the recipient of the transferred data that such recipient will take sufficient precautions to protect the privacy of the data subjects and will not transfer the data to anyone else. In addition, an international transfer may not be made unless one (or more) of the criteria set forth below are met.

8.2 Legal basis for international data transfers

Pursuant to the Data Transfer Regulations, the following constitute the legal basis for international transfers of data:
- the data are transferred to a country the laws of which ensure that the transferred data are protected to a degree no less than that accorded by Israeli law and incorporate the following principles: (i) data must be gathered and processed legally and fairly; (ii) data shall be held, used and transferred solely for the purpose for which they were received; (iii) stored data shall be correct and current; (iv) data subjects shall have the right to view and correct the data; and (v) proper security precautions should be implemented to protect the data;
- the data subject has consented to the transfer;
- the transfer is critical to the subject's health and he or she is unable to give consent;
- the data are transferred to a corporation in which the owner of the Israeli-based database has a controlling interest (ie over 50 per cent) and the corporation has undertaken to maintain the privacy of the data;
- the recipient undertakes toward the owner of the Israeli-based database to uphold the laws regarding the holding and using of data applying to databases located in Israel;
- the data have been lawfully publicised;
- transfer of data is necessary for the benefit or the security of the public;
- transfer of data is required under Israeli law; or
- data are transferred to a database in a country: (i) which is a party to the

Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the Convention); (ii) which receives data from other European Union member countries under the same terms and conditions (which has been interpreted by the Registrar to include entities participating in the US Safe Harbour scheme) ; and/or (iii) which, according to a declaration issued by the Israeli Registrar, has a privacy protection authority with which the Registrar has reached a co-operative understanding.

8.2.1 Legal basis for international agreements.

As mentioned above, under the Data Transfer Regulations, the transfer of data outside the State of Israel is strictly prohibited unless the database owner secures the written undertaking of the recipient of the transferred data that such recipient will take sufficient precautions to protect the privacy of the data subjects and will not transfer the data to anyone else. In addition, as described above, a transferee undertaking toward the owner of the Israeli-based database to uphold the laws regarding the holding and using of data applying to databases located in Israel can also serve as legal basis for the international transfer of data. The European Commission's standard contractual clauses can be used where they are revised to incorporate the mandatory Israeli provisions described above.

8.2.2 Binding corporate rules

Not applicable.

8.2.3 Safe Harbour

Not applicable.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Personal information contained in databases is considered confidential, and a person may be subjected to five years' imprisonment for disclosing data obtained by virtue of his or her position as an employee, manager or holder in respect of a database, except for the purpose of performing his or her duties or implementing the Privacy Law or under a court order in connection with legal proceedings.

9.2 Security

The Privacy Law contains specific provisions regarding the security of data in databases. 'Data security' is defined as *'the protection of the integrity of data, or protection of the data against exposure, use or copying, all when done without due permission'*. The phrase 'integrity of data' is defined to mean that the information in the database is identical *'to the source from which it was derived, without having been changed, delivered or destroyed without due permission'*. Owners, holders and managers of databases are each responsible for data security.

Pursuant to the Data Possession Regulation, maintaining database security

includes: (i) ensuring physical protection of the automatic data processing system and infrastructure; (ii) setting administrative procedures regarding permitted access to the data and instructions regarding their collection, verification, processing and distribution (such procedures are also applicable to anyone providing external services to the database owner); (iii) granting access authorisation to the database and restricting the access of authorised users in accordance with the instructions of the Data Transfer Committee (a committee to be appointed by each public body); (iv) preparation of an updated list of authorised users according to the various degrees of authorisation; (v) ensuring the authorised users sign undertakings to maintain the confidentiality of the data and to uphold the Data Transfer Committee instructions; (vi) establishing operating procedures for the system, including data security and protection for the integrity of data; (vii) implementing reasonable security measures, in accordance with the level of sensitivity of the data, that will prevent intentional or accidental access to the system by a user beyond the areas of data permitted to him; and (viii) establishing controls to reveal damage to the integrity of the data and repair defects.

Additional requirements apply in respect of 'restricted data' and include the following: (i) the database must be administered according to guidelines for security and supervision of physical storage of the data (including a chapter governing any external service provider performing services such as data entry, data processing, etc); (ii) any print-outs containing restricted information that are distributed by a public body must state on each page that the information contains data protected by law and that unauthorised distribution is a crime; (iii) the database manager must maintain a list of the users of the restricted information, and a list of those permitted access to the data (including their identification numbers, access codes and the type of information to which they are permitted access); the access codes must be changed periodically and not less than once every six months or upon a change of employees; (iv) restrictions on access to the back-up copies of restricted information; (v) documents and magnetic records of intermediate processing activities must be burned, shredded or otherwise destroyed; and (vi) the database manager must keep a journal of atypical events and save it for three years.

Under Directive 1-2010 published by the Registrar, where data subjects can remotely access personal data stored in a database, the database owner must implement a verification process that requires the data subject to submit at least one item of data which should only be known to the data subject. The number of verification items required should rise in accordance with the sensitivity of the data, or alternatively, other measures could be employed, such as identity verification by means of a SIM card, cellular phone or biometric characteristic. Failure to correctly assess the sensitivity of the data and adjust the requirements accordingly constitutes a breach of data security obligations.

The Privacy Protection Council (an entity established by the Minister of Justice to advise on matters related to the Privacy Law and to provide guidance to the Registrar and the Israel Chamber of System Analysts (a

nonprofit IT and information systems professional organisation) have issued a set of (non-binding) guidelines intended to assist database managers in implementing the Privacy Law - they can be accessed at: *www.justice.gov.il/NR/rdonlyres/C0681561-6CD4-4A6E-AE85-E2ABACC2C171/0/parta.pdf*.

9.3 Data security breach notification

Data security breach notification is not required under the current law; however, if the draft Protection of Privacy Regulations (Information Security in Databases) 2010 are enacted as law, they will require the data security officer to document events of a possible breach of the database (if possible, by automatic documentation), and the security policy of a medium to high security database would have to include provisions for the report to the database owner of security breaches. ILITA's Directive 2-2011 on outsourcing requires service providers to provide immediate breach notifications of possible security failures to the database owner (see section 3.5 above).

9.4 Data protection impact assessments and audits.

Such assessments and audits are recommended in certain circumstances pursuant to the Directive and the non-binding guidelines published by the Registrar (see sections 3.5, 3.6.1 and 3.6.2 above).

10. ENFORCEMENT, SANCTION, REMEDIES AND LIABILITY

10.1 Enforcement action

The Registrar has the authority to suspend or rescind database registrations due to a failure to comply with database laws. The Registrar has also issued notices of non-compliance.

10.2 Sanction

The Registrar may impose the following administrative fines:

- using, holding or managing an unregistered database requiring registration in breach: NIS 2,000;
- use of database information for purposes differing from those for which the database was registered: NIS 5,000;
- delivering false information in a database registration application: NIS 2,000;
- failing to deliver information or delivering false information in a notice soliciting information for inclusion in a database: NIS 3,000;
- failing to comply with data subjects' inspection rights: NIS 3,000;
- granting access to a database to someone not authorised under the written agreement between data subject and database owner: NIS 3,000;
- failing to deliver documents or an affidavit to the Registrar where required by a holder of at least five databases: NIS 2,000;
- failing to appoint a security officer for data security for databases which are so required by law: NIS 3,000;
- managing or possessing a database used for direct mail services without designation such use in the database registration: NIS 3,000;
- managing or possessing a database used for direct mail services 17E

without properly tracking of sources of information used: NIS 2,000;
- managing or possessing a database used for direct mail services without properly notifying database subjects or responding to requests for removal: NIS 3,000.

Pursuant to the Administrative Offence Regulations (Administrative Fine – Protection of Privacy) 2004, a five-fold fine for every type of violation can be imposed upon a corporation. For continuing violations, one-tenth of the fine can be imposed for each day of violation after service of warning of the breach. As mentioned above, draft legislation, if enacted, would substantially increase fines which the Registrar is entitled to impose.

10.3 Examples of recent enforcements of data protection rules

In recent years, ILITA has issued administrative fines for database violations, issued notices of non-compliance and de-registered databases and ordered the destruction of database contents. Situations in which administrative fines have been imposed include:

- failure to include full details in a notice for solicitation of database information;
- violation of direct mail provisions of the Privacy Law;
- illegal trading in databases;
- use of an illegal online database for marketing purposes;
- use of database information for purposes other than those for which the database (a voter registry) was established and delivering of false details in a registration application;
- use of information provided by a customer in order to solicit him for other purposes.

The amount of fines imposed ranged from several thousand NIS to NIS 258,000.

10.4 Judicial remedies

An infringement of privacy is actionable as a civil wrong pursuant to Privacy Law, and a claimant may obtain monetary compensation or injunctive relief. Violations of Privacy Law sections 2(7), 2(9), 2(10) or 2(11) (ie, infringing an obligation of secrecy laid down by law in respect of a person's private affairs; using, or passing on to another, information on a person's private affairs other than for the purpose for which it was given, publishing or passing on anything that was obtained by way of an infringement of privacy under certain provisions of the Privacy Law or publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain) are subject to five years' imprisonment. No civil or criminal action may be brought for violations with no real significance.

A court may award damages amounting to NIS 50,000 without proof of damages for breach of privacy rights, and damages may be doubled where the privacy infringement was with intent to harm.

10.5 Class actions.

The Privacy Law does not expressly authorise class action claims for privacy

or database violations. However, the Class Action Law 2006 provides a closed list of circumstances under which class actions may be brought. For example, class actions may be brought against a vendor, supplier, manufacturer, importer or marketer of a product or service, with regard to the relationship between it and a customer, and a number of privacy and database-related class actions have been brought in Israeli courts under this provision. There are additional grounds for class actions which may be relevant to the data protection context as well (for example, class action claims are permitted under certain circumstances against a bank or insurer).

10.6 Liability

Violators may be subjected to five years' imprisonment for disclosing data obtained by virtue of his position as an employee, manager or holder in respect of a database, except for the purpose of performing his duties or implementing the Privacy Law or under a court order in connection with legal proceedings.

Violators may be subjected to one year's imprisonment for breach of the following obligations regarding databases: (i) managing, possessing or using a database in breach of Privacy Law (ie, the obligations to register certain databases); (ii) delivering false details in an application for registration of a database in violation of Privacy Law ; (iii) failing to deliver details or delivering false details in a notice attached to a request for information under Privacy Law section 11; (iv) failing to comply with the provisions of Privacy Law, regarding the right to inspect information kept in a database, or failing to amend a database in accordance with the requirements of Privacy Law ; (v) granting access to a database in breach of Privacy Law, or failing to deliver documents or an affidavit to the Registrar in accordance with the provisions of the Privacy Law; (vi) failing to appoint a security officer for data security as required by the Privacy Law; (vii) managing or possessing a database used for direct mail services in breach of the provisions of the Privacy Law regarding direct mail; and (viii) delivering information in breach of the Privacy Law (regarding public bodies).

These are strict liability offences, as neither criminal intent nor negligence need be proven.

There are no provisions specifically setting out rights to compensation for damage suffered as a result of inaccurate data. However, since breaches of the Privacy Law are actionable as civil torts, compensation for damage arising from use of inaccurate data maintained in violation of the Data Possession Regulations could theoretically be awarded.

In addition to providing that an infringement of privacy is actionable as a civil wrong, the Privacy Law also specifies that an act or omission in breach of the provisions of Chapter Two (protection of privacy in a database) or Chapter Four (delivery of information by public bodies), or in breach of any regulations issued pursuant to the Privacy Law, is a civil wrong under the Civil Wrongs Ordinance (new version). This provision was added in order to ensure that even omissions such as a failure to ensure data security would also be actionable as a civil wrong.

Italy

CBA Studio Legale e Tributario
Gerolamo Pellicanò & Giovanna Boschetti

1. LEGISLATION

1.1 Name/title of the law

The collection and protection of personal data in Italy is governed by the Legislative Decree no. 196 dated 30 June 2003 – *Codice in materia di protezione dei dati personali* (Personal Data Protection Code) (the Code) implementing the Data Protection Directive 95/46/EC (the Directive), as subsequently amended. The Code substituted the previous law in force, n. 675/1996.

Also the Constitution of the Italian Republic of 27 December 1947 provides relevant rules on the general right of privacy, in particular Article 2 establishing that 'the Republic recognises and guarantees the inviolable rights of a person, as individual and in the community where he expresses its personality […]' and Article 15 establishing that 'the freedom and secrecy of correspondence and any other form of communication is inviolable'.

1.2 Pending legislation

There is no pending legislation.

1.3 Scope of the law

1.3.1 The main players

The main players are:

- the 'data controller' shall mean any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters;
- the 'data processor' shall mean any natural or legal person, public administration, body, association or other agency that processes personal data on the data controller's behalf;
- 'persons in charge of processing' shall mean the natural persons that have been authorised by the data controller or processor to carry out processing operations;
- the 'data subject' shall mean any natural or legal person, body or association that is the subject of the personal data.

The definition of 'third parties' is not provided in the Code.

1.3.2 Types of data

The Code covers personal data relating both to natural persons and legal persons (eg companies).

The Code contemplates the following main categories of data:

- 'personal data' shall mean any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number;
- 'identification data' shall mean personal data allowing a data subject to be directly identified;
- 'sensitive data' shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade unionist character, as well as personal data disclosing health and sex life;
- 'judicial data' shall mean personal data disclosing the measures referred to in section 3(1), letters (a) to (o) and (r) to (u), of Presidential Decree no. 313 of 14 November 2002 concerning the criminal record office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either defendant or the subject of investigations pursuant to sections 60 and 61 of the Criminal Procedure Code.
- 'anonymous data' shall mean any data that either in origin or on account of their having been processed cannot be associated with any identified or identifiable data subject.

1.3.3 Types of acts/operations

The Code covers the 'processing' of personal data, defined as any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilisation, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank; a 'data bank' is defined as any organised set of personal data, divided into one or more units located in one or more places.

1.3.4 Exceptions

The Code shall only apply to the processing of personal data carried out by natural persons for exclusively personal purposes if the data are intended for systematic communication or dissemination (while the provisions concerning liability and security shall apply in any case).

Furthermore, the processing of personal data relating to legal persons, companies, corporations or associations conducted solely in the context of relationships existing between the same parties for administrative and accounting purposes is not subject to the Legislative Decree. A data processing operation for administrative and accounting purposes is defined as 'any processing operation that is related to the performance of organisational, administrative, financial and accounting activities irrespective of the nature of the processed data. The said purposes apply,

in particular, to in-house organisational activities, the activities aimed at fulfilling contractual and pre-contractual obligations, managing employer-employee relationships, keeping accounting records, and implementing the legislation on taxation, trade unions, social security and welfare, and occupational health and safety'.

1.3.5 Geographical scope of application

The Code shall apply to the processing of personal data, including data held abroad, where the processing is performed by any entity established either in the state's territory or in a place that is under the state's sovereignty.

The Code also applies to the processing of personal data that is performed by an 'entity' (which can be interpreted in the light of the Directive, as the 'data controller') established in the territory of a country outside the European Union, where said entity makes use in connection with the data processing of equipment, whether electronic or otherwise, situated in the state's territory, unless such equipment is used only for purposes of transit through the territory of the European Union. In such a case, the data controller shall designate a representative established in the state's territory with a view to implementing the provisions concerning processing of personal data.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

The Data Protection Authority (*Garante per la protezione dei dati personali*) (the Garante).
Address: Piazza di Monte Citorio n. 121, 00186 Rome, Italy
T: (+39) 06.696771
F: (+39) 06.69677.3785
E: garante@garanteprivacy.it
W: *www.garanteprivacy.it*

2.1 Role and tasks

The Garante is an authority acting fully autonomously and independently in its decisions and assessments.

The main tasks to be discharged by the Garante, also with the help of the Office operating under its authority (supervised by a General Secretary) and in compliance with the Code, consists of:

- verifying whether data processing operations are carried out in compliance with laws and regulations in force as well as with the relevant notification *vis-à-vis* the Garante, also in case of termination of processing operations and with regard to the retention of traffic data;
- receiving reports and complaints, and taking steps as appropriate with regard to the complaints lodged by data subjects or the associations representing them;
- ordering data controllers or data processors, also ex officio, to adopt

such measures as are necessary or appropriate for the processing to comply with the specific provisions of the Code;
- prohibiting, also ex officio, unlawful or unfair data processing operations, in whole or in part, or blocking such processing operations, and taking other measures as provided for by the legislation applying to processing of personal data;
- encouraging the adoption of codes of conduct provided for in the Code. In particular, the following codes of conduct have been adopted: (i) for processing of personal data in the exercise of journalistic activities; (ii) code of conduct and professional practice regarding the processing of personal data for historical purposes; (iii) for processing of personal data for statistical purposes within the framework of the SI.STA.N. (national statistical system); (iv) processing of personal data for statistical and scientific purposes; (v) code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments; and (vi) code of practice applying to the processing of personal data performed with a view to defence investigations;
- drawing the attention of parliament and government to the advisability of legislation as required by the need to protect personal data, also in the light of sectoral developments;
- giving opinions whenever required;
- raising public awareness of the legislation applying to personal data processing and the relevant purposes as well as of the data security measures;
- referring to the prosecutor information on facts and/or circumstances amounting to offences to be prosecuted ex officio, which it has come to know either in discharging or on account of its duties;
- keeping the register of processing operations as drawn up on the basis of the notifications of processing;
- drawing up an annual report on the activity performed and implementation of the Code, which shall be submitted to parliament and the government by 30 April of the year following that to which the report refers.

The Garante also discharges supervisory or assistance tasks concerning personal data processing as provided for by acts ratifying international agreements and conventions or else by Community regulations, and co-operates with other independent administrative authorities in the performance of relevant duties; to that end, the Garante may also invite representatives from another authority to take part in its meetings, or else be invited to take part in the meetings of another authority, and contribute to the analysis of issues of common interest. The Garante may also request the cooperation of specialised staff from another authority.

The Prime Minister and every Minister consult the Garante when drawing up regulations and administrative measures that are liable to produce effects on the matters regulated by the Code; the Garante's opinion shall be rendered in the cases at stake within 45 days of receiving the relevant

request.

That stated it has to be highlighted that the competence over any disputes concerning the application of the provisions of the Code, including those related either to provisions issued by the Garante with regard to personal data protection or to the failure to adopt such provisions, shall lie with the judicial authorities.

2.2 Powers

In discharging its tasks, the Garante may request the data controller, the data processor, the data subject or a third party to provide information and produce documents; the inquiries shall be carried out by staff from the Office though the Garante may also avail itself, if necessary, of the cooperation of other state agencies.

The Garante may order that data banks and filing systems (as defined by Article 3 of Directive 95/46/CE) be accessed and audits on the spot be performed as regards premises where the processing takes place or investigations are anyhow to be carried out with a view to checking compliance with personal data protection regulations.

2.3 Priorities

Every year, by 30 of April, the Garante draws up a report on the activity performed which is submitted to the parliament and to the government. The areas on which its inspection activity will focus are identified by the Garante at the beginning of the year.

The inspection plan for 2011 identified in particular the following areas on which the Garante's inspection activity will focus: private investigators; computer services (particularly those provided through 'cloud computing'); banks and credit cards; marketing; telemarketing; (including via SMS, email and massive use of junk faxes); customer care; debt collection companies; and social security institutions.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

The Code provides that processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent; the data subject's consent may refer either to the processing as a whole or to one or more of its operations.

The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information provided for by law.

According to the Garante, 'freely given, specific and informed' means that the data subject may not be put under pressure to say 'yes' to the data processing, that consent must relate to precisely defined data processing and that the data subject must have received all useful information concerning the contemplated data processing.

3.1.2 Form

Consent shall be given in writing if the processing concerns sensitive data (this is different from consent to non-sensitive personal data, which can be given freely but with the data controller eventually required to give, *ad probationem*, evidence in written form of the obtained consent).

3.1.3 In an employment relationship

There being some concerns as to whether an employee's consent can be freely given due to the nature of the subordinated relationship, personal data may be processed without consent if it is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also with regard to occupational and population hygiene and safety and to social security and assistance purposes. Consent is not required for the processing of personal data contained in a curriculum vitae sent by candidates.

3.2 Other legal grounds for data processing

Personal data may be processed without consent, if the processing:

- is necessary to comply with an obligation imposed by a law, regulations or Community legislation;
- is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract, or else if the data are contained in a curriculum vitae sent by the data subject;
- concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and Community legislation with regard to their disclosure and publicity;
- concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;
- is necessary to safeguard life or bodily integrity of a third party;
- except for dissemination, is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary by complying with the legislation in force concerning business and industrial secrecy, dissemination of the data being ruled out;
- is necessary to pursue a legitimate interest of either the data controller or a third party recipient in the cases specified by the Garante on the basis of the principles set out under the law, unless said interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests, dissemination of the data being ruled out;
- except for external communication and dissemination, is carried out by non-profit associations, bodies or organisations, recognised or not, with

regard either to entities having regular contact with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with an information notice provided for;

- is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice or else exclusively for historical purposes in connection either with private archives that have been declared to be of considerable historical interest or with other private archives pursuant to the provisions made in the relevant codes;
- with regard to data contained in the curriculum vitae of job applicants, if the data are processed in compliance with an obligation imposed by a law, regulations or Community legislation;
- except for dissemination and without prejudice to the rules concerning direct marketing, involves the communication of data between companies, organisations or associations with holding subsidiaries or affiliate companies, or with companies under common control, as well as consortia, business networks, clusters and joint ventures with entities belonging to them, for administrative and accounting purposes as long as the data subjects are informed about these purposes.

The data processing of sensitive date requires, further to the written consent of the data subject, the Garante's authorisation.

The sensitive data are the object of processing without consent from the data subject, but with the Garante's authorisation:

- if the processing is carried out for specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements by not-for-profit associations, bodies or organisations, whether recognised or not, of political, philosophical, religious or trade unionist nature, including political parties and movements, with regard to personal data concerning members and/or entities having regular contact with said associations, bodies or organisations in connection with the aforementioned purposes, provided that the data are not communicated or disclosed outside and the bodies, associations or organisations lay down suitable safeguards in respect of the processing operations performed by expressly setting out the arrangements for using the data through a resolution that shall be made known to data subjects at the time of providing the information;
- if the processing is necessary to protect a third party's life or bodily integrity;
- if the processing is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefore. Said claim must not be overridden by the data subject's claim, or else must consist in a personal right or another fundamental, inviolable right or freedom, if the data can disclose health and sex life;

- if the processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also with regard to occupational and population hygiene and safety and to social security and assistance purposes, to the extent that it is provided for in the Garante's authorisation and subject to the requirements of the code of conduct and professional practice.

3.3 Direct marketing and cookies

The Code provides that communications for the purposes of direct marketing using different means shall be allowed with (and, when concerning data taken from public registers, lists, documents or records that are publicly available, without) the express consent of the data subject.

The use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the user's consent; this rule shall also apply to electronic communications performed by email, facsimile, MMS- or SMS-type messages or other means for the purposes of marketing.

Furthermore, processing by telephone or by mail of the data contained in directories of subscribers for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys, shall be allowed in respect of any entities that have not exercised their right to object by using the established Public Opt-Out Register (managed by a public body). This rule also applies to consumers.

Where a data controller uses, for direct marketing of its own products or services, electronic contact details for email or mail, supplied by a data subject in the context of the sale of a product or service, said data controller has to request the data subject's consent unless the services are similar to those that have been the subject of the sale and the data subject, after having been adequately informed, does not object to said use either initially or in connection with subsequent communications.

It is prohibited to use an electronic communication network to gain access to information stored in the terminal equipment of a subscriber or user, to store information or monitor operations performed by that user.

3.4 Data quality requirements

Personal data undergoing processing shall be:

- processed lawfully and fairly;
- collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes;
- accurate and, when necessary, kept up to date;
- relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed;
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

Personal data that are processed in breach of the relevant provisions concerning the processing of personal data may not be used.

3.5 Outsourcing

When outsourcing data processing activities, the data controller is required to appoint the subject (or subjects) carrying out the outsourcing activities as a data processor (or data processors).

The data processor must be selected from among those entities that can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to the data processing, including related to security matters. The tasks committed to the data processor must be detailed in writing by the data controller and the data processor must abide by the instructions given by the data controller when carrying out the processing. The data controller must supervise thorough compliance with both said instructions and the correct processing, comply with the security aspects and also carry out regular controls.

3.6 Email, internet and video monitoring

3.6.1 General rules

Neither the monitoring of email and internet nor the use of surveillance cameras are regulated in the Code. Nevertheless, while the use of email and internet in the workplace is regulated by the Workers' Charter (Law n. 300/1970, which prohibits all forms of remote control), the general rules on video surveillance are set out in the Garante's last decision on 'General measures on video surveillance' dated 8 April 2010.

According to this decision, the following is deemed necessary:

- the processing of data via video surveillance must comply with a so-called 'balancing of interest' criterion and requires free and explicit consent by the data subject;
- the proportionality principle must be respected, when selecting filming arrangements and location (eg the use of fixed or pan-tilt cameras with or without zooming) as well as in the course of the processing of data, which must in any case be relevant and not excessive in connection with the purposes to be achieved;
- every IT system, including the software, must be designed in such a way so as not to use data related to identifiable individuals if the purposes of the processing can be achieved by only relying on anonymous data (eg by configuring the software to only enable a bird's-eye view in monitoring road traffic without zooming in on images and making individuals identifiable). This is a requirement arising out of the data minimisation principle, whereby IT systems and software should be configured in order to minimise the use of personal data.

Data subjects should always be informed (using the model information notice provided by the Garante) that they are about to enter an area under video surveillance; this also applies to events and/or public shows (eg concerts, sports events, etc). To that end, the model information notice:

- should be posted outside the area covered by the surveillance cameras, but it can be as close as possible to them and need not be posted on the devices themselves;
- should be formatted and posted in such a way as to be clearly visible regardless of light conditions, including during the night operation of the video surveillance;
- may include a symbol and/or graphics that should be immediately and easily understandable and may also be different to specify whether the images are only viewed or are also recorded.

In the said provision specific rules have also been set out for specific fields (such as in the workplace, at hospital, at school) and needs (public order, street security monitoring).

Any data that are collected via video surveillance must be protected through suitable security measures that should minimise the risk of their destruction or loss (whether by accident or not) unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected including with regard to the transmission of the images.

3.6.2 Employment relationship

According to the latest Garante decision 'General decision on video surveillance' dated 8 April 2010, the prohibition against monitoring of employees' activities in the workplace should be complied with. Accordingly, it is forbidden to deploy equipment that is specifically intended for the above purposes. No surveillance should take place in order to check compliance with duties applying to working hours and appropriate discharge of workplace tasks – eg by tilting cameras to film employees' badges. Additionally, occupational safeguards should be abided by if video surveillance proves necessary because of organisational and/or production requirements or else for occupational safety purposes. Under Article 4 of Law no. 300/1970, any devices and equipment 'that may give rise to the mere possibility of remotely monitoring employees' activities may only be installed in agreement with the trade union representatives in the given business or, failing these, with the internal labour committee. Failing such agreement, the Labour Inspectorate shall step in at the employer's request and lay down, where necessary, the arrangements applying to use of the said devices and equipment.'

The above safeguards should be respected both indoors and in any other workplace environment – eg in building yards, or for the cameras installed on board passenger vehicles or taxi cabs. Those cameras should not film the drivers continuously, and any images collected to ensure security and counter criminal offences may not be used to check – albeit indirectly – the relevant employees' activities.

Failure to comply with the above requirements results in the imposition of criminal and administrative sanctions.

Using video surveillance systems to purposely monitor employees remotely and/or investigate employees' opinions is a criminal offence under

the Code.

On a different note, the case of TV cameras filming workplaces and employees to document activities and/or operations exclusively in order to provide information to the general public and/or in connection with institutional and/or corporate communication initiatives may be equated to a transitional processing operation for the purpose of the occasional publication of articles, papers and other intellectual works. Accordingly, the provisions on journalistic activities contained in the Code are applicable, without prejudice to the limitations placed on press freedom to ensure confidentiality, the need to comply with the code of conduct related to journalistic activities, and the employees' right to protect their own images by objecting, on legitimate grounds, to the dissemination of such images.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers are responsible for informing the data subjects about the processing of personal data relating to them.

4.2 What

The data subject as well as any entity from which personal data are collected shall be preliminarily informed, either orally or in writing, as to:

- the purposes and modalities of the processing for which the personal data are intended;
- the obligatory or voluntary nature of providing the requested data;
- the consequences if (s)he fails to reply;
- the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;
- the rights of the data subject provided in the Code, such as the updating, rectification, integration, erasure, anonymisation of the data, or blocking of data that have been processed unlawfully;
- the identification data concerning the data controller and, where designated, the data controller's representative in the state's territory.

The data controller is exempt from providing the above information if:

- the data subject is already aware of the information;
- providing this information proves impossible or would require a disproportionate effort; or
- recording or disclosure of the personal data is expressly laid down by law.

4.3 When

The information should be provided before the data collection.

Whenever the personal data are not collected from the data subject, the information above, also including the categories of processed data, shall be provided to the data subject at the time of recording such data or, if their communication is envisaged, no later than when the data are first

communicated.

4.4 How

The information could be provided either orally or in writing.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

A data subject shall have the right to obtain, from the data controller and/or data processor, confirmation as to whether or not personal data concerning him exist, regardless of their being already recorded, and communication of such data in an intelligible form.

A data subject shall have the right to be informed:

- of the source of the personal data; of the purposes and methods of the processing;
- of the logic applied to the processing, if the latter is carried out with the help of electronic means;
- of the identification data concerning the data controller, data processors and the representative eventually designated;
- of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the state's territory, data processor(s) or person(s) in charge of the processing.

In addition, data subjects shall have the right to obtain:

- where interested, integration of the data (meaning the possibility of implementation of further information about the data subject);
- certification to the effect that the operations above have been notified, as also related to their contents, to the entities to which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.

The right to access the data processed may be exercised by the data subject by making a request to the data controller or data processor without formalities, also by means of a person in charge of the processing.

The right to access may also be exercised by sending a request to the data controller by means of a registered letter, facsimile or email.

5.1.2 Exceptions

The right to access may not be exercised by making a request to the data controller or processor, or else by lodging a complaint, in a few specific cases, if the personal data are processed:

- pursuant to the provisions of decree-law no. 143 of 3 May 1991, as converted, with amendments, into Act no. 197 of 5 July 1991 and subsequently amended, concerning money laundering;
- pursuant to the provisions of decree-law no. 419 of 31 December 1991, as converted, with amendments, into Act no. 172 of 18 February 1992 and subsequently amended, concerning support for victims of extortion;

- by parliamentary inquiry committees set up as per Article 82 of the Constitution;
- by a public body other than a profit-seeking public body, where this is expressly required by a law for purposes exclusively related to currency and financial policy, the system of payments, control of brokers and credit and financial markets and protection of their stability;
- for the period during which performance of the investigations by defence counsel or establishment of the legal claim might actually and concretely be prejudiced;
- by providers of publicly available electronic communications services in respect of incoming phone calls, unless this may actually and concretely be prejudicial to the performance of the investigations by defence counsel as per Act no. 397 of 7 December 2000;
- for reasons of justice by judicial authorities at all levels and of all instances as well as by the Higher Council of the Judiciary or other self-regulatory bodies, or else by the Ministry of Justice;
- without prejudice to Act no. 121 of 1 April 1981 regarding the new system of public security administration.

5.1.3 Deadline

The data subject can exercise the right to access at any time; the request may be worded freely without any constraints and may be renewed at intervals of not less than 90 days, unless there are well-grounded reasons.

No deadline is provided for a suitable response by the data controller.

5.1.4 Charges

The data subject may not be charged for exercising his right to access. Where it is not confirmed that personal data concerning the data subject exist, further to a request, the data subject may be charged a fee which shall not be in excess of the costs actually incurred for the inquiries made by the data controller in the specific case.

5.2 Rectification

5.2.1 Right

Any data subject has the right to obtain from the data controller and / or the data processor the rectification of incorrect personal data relating to him. Furthermore, exercise of the right to obtain rectification may be permitted with regard to data of non-objective character on the condition that it does not concern rectification of or additions to personal evaluation data in connection with judgments, opinions and other types of subjective assessment, or else the specification of policies to be implemented or decision-making activities by the data controller.

The same rules as provided for regarding the right to access apply.

5.2.2 Exceptions
The same exceptions as for the right to access apply (see section 5.1.2 above).

5.2.3 Deadline
The same rules provided for regarding the right to access apply (see section 5.1.3 above).

5.2.4 Charges
The same rules provided for regarding the right to access apply (see section 5.1.4 above).

5.3 Erasure
5.3.1 Right
A data subject shall have the right to obtain, from the data controller and/or the data processor, the erasure of data that have been processed unlawfully, including data the retention of which is unnecessary for the purposes for which they have been collected or subsequently processed.

5.3.2 Exceptions
The same exceptions as for the right to access apply (see section 5.1.2 above).

5.3.3 Deadline
The same rules provided for regarding the right to access apply (see section 5.1.3 above).

5.3.4 Charges
The same rules provided for regarding the right to access apply (see section 5.1.4 above).

5.4 Blocking
5.4.1 Right
Any data subject has the right to ask the data controller and/or the data processor to block any use of personal data relating to him, under the same conditions provided with reference to the right to erasure.

5.4.2 Exceptions
The same exceptions as for the right to access apply (see section 5.1.2 above).

5.4.3 Deadline
The same rules provided for regarding the right to access apply (see section 5.1.3 above).

5.4.4 Charges
The same rules provided for regarding the right to access apply (see section 5.1.4 above).

5.5 Objection

5.5.1 Right

A data subject shall have the right to object, in whole or in part:

- on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection;
- to the processing of personal data concerning him/her, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys.

5.5.2 Exceptions

The same exceptions as for the right to access apply (see section 5.1.2 above).

5.5.3 Deadline

The same rules provided for regarding the right to access apply (see section 5.1.3 above).

5.5.4 Charges

The same rules provided for regarding the right to access apply (see section 5.1.4 above).

5.6 Automated individual decisions

5.6.1 Right

No judicial or administrative act or measure involving the assessment of a person's conduct may be based solely on the automated processing of personal data aimed at defining the data subject's profile or personality.

5.6.2 Exceptions

The data subject may challenge any other decision that is based on the automated processing of personal data, unless such decision has been taken for the conclusion or performance of a contract, further to a proposal made by the data subject or on the basis of adequate safeguards laid down either by the Code or in a provision issued by the Garante.

5.6.3 Deadline

No deadline is provided.

5.6.4 Charges

The data subject may not be charged for exercising his right.

5.7 Other rights

5.7.1 Right

There are no other rights contemplated in the Code.

5.7.2 Exceptions

Not applicable.

5.7.3 Deadline
Not applicable.

5.7.4 Charges
Not applicable.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who
The data controller shall notify the Garante of the data processing in the cases listed in section 6.1.2 below.

6.1.2 What
A data controller shall notify the processing of personal data he/she intends to perform if said processing concerns:

(a) genetic data, biometric data, or other data disclosing the geographic location of individuals or objects by means of an electronic communications network;

(b) data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure;

(c) data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade union character;

(d) data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users;

(e) sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys;

(f) data stored in ad hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

6.1.3 Exceptions
Notification shall not be required if the processing mentioned in section 6.1.2 above concerns the activity carried out by general practitioners and/or freely chosen paediatricians, as the relevant functions are typical of their professional relationships with the National Health Service.

Furthermore, there is no notification requirement:

- regarding the data described in section 6.1.2(a) above, for (i) non-systematic processing operations of genetic and/or biometric data,

subject to certain conditions; (ii) processing of genetic and/or biometric data carried out in the exercise of the legal profession with regard to such data and operations as are necessary to carry out the investigations by defence counsel, and anyhow to establish or defend a legal claim also concerning a third party, on condition that said claim is not overridden by that of the data subject and the data are only processed with a view to said purposes and for no longer than is absolutely necessary; (iii) processing of data disclosing the geographic position of air, sea, and ground transportation means, where it is only carried out for the purpose of transportation security.

- regarding the data described in section 6.1.2 (b) above, for the processing of data suitable for disclosing health and sex life where it is performed by health care professionals, whether jointly or not with other health care professionals acting as data controllers of said processing (i) for certain specified medical purposes, subject to conditions or; (ii) exclusively for the purpose of monitoring health care expenditure or else fulfilling regulatory obligations in respect of occupational and population health and safety.
- regarding the data described in section 6.1.2 (c) above, for the processing of data suitable for disclosing workers' psychological sphere: (i) where it is performed by associations, bodies or organisations of trade unionistic nature exclusively to fulfil specific obligations and/or duties as set out in employment and/or social security legislation, also concerning the disabled persons' right to employment; (ii) where it is performed by not-for-profit associations, bodies or organisations, recognised or not, of a political, philosophical or religious nature with regard to data concerning their own employees and/or collaborators exclusively in order to fulfil specific obligations as set out in employment and/or social security legislation.
- regarding the data described in section 6.1.2 (d) above, for the processing of personal data: (i) that is not grounded exclusively on an automated processing operation aimed at defining professional profiles, where said processing is carried out exclusively for occupational purposes or else for the purpose of managing the employer-employee relationship (except for the sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys), (ii) that is not grounded exclusively on an automated processing operation aimed at defining an investor's profile, where said processing is carried out exclusively in order to fulfil specific obligations set out in financial brokerage legislation; (iii) that is related to the use of electronic markers or similar devices whether installed or temporarily stored, in a non-persistent manner, on a user's terminal equipment, as consisting exclusively in the transmission of session IDs pursuant to the applicable regulations for the sole purpose of facilitating access to the content of internet sites.
- regarding the data described in section 6.1.2 (e) above, for the

processing of sensitive data carried out: (i) for the sole purpose of personnel selection exclusively on behalf of entities belonging to the same company and/or banking group; (ii) by public entities exclusively in order to fulfil specific obligations and/or duties as set out in employment and/or labour market legislation; (iii) by trade associations and/or organisations for the sole purpose of carrying out sample surveys with regard to data concerning membership of said associations and/or organisations.

- regarding the data described in section 6.1.2 (f) above, for the processing of personal data: (i) carried out by public entities to keep public registers or else publicly available lists; (ii) that are stored in data banks used to keep in touch with a data subject in connection with the provision of goods or services, or else to comply with accounting and/or tax requirements as also related to breach of contract, factoring of receivables and litigation involving said data subject; (iii) that are stored in data banks used by public and/or private entities exclusively to fulfil regulatory obligations concerning employment, social security, or assistance; (iv) that are stored in data banks used by public bodies exclusively with a view to keeping and executing instruments, provisions and documents related to levying of taxes, imposition of administrative sanctions, or granting of licences, concessions, and authorisations; (v) related to images and/or sound as temporarily stored for the sole purpose of securing and/or protecting individuals and/or property; (vi) carried out pursuant to law by the entities authorised thereto in connection with such operations and data as are necessary exclusively with a view to collective suretyship guarantees (so-called *confidi*) and any services that are related and/or instrumental thereto.

With the decision dated 23 April 2004 the Garante gave further clarifications on the cases exempted from notification noted above.

6.1.4 When

The notification of processing operations have to be submitted to the Garante in advance of the processing and once only, regardless of the number of operations to be performed and the duration of the processing.

A new notification shall only have to be submitted either prior to termination of processing operations or in connection with the modification of any of the items to be specified in the notification.

6.1.5 How

A notification may concern one or more processing operations for related purposes. It shall only be effective if it is transmitted via the Garante's website by using the online form, which shall contain the following information:

- information to identify the data controller and, where appropriate, his/her representative, as well as the arrangements to identify the data processor if one has been appointed;
- the purpose(s) of the processing;

- a description of the category/categories of data subject and the data or data categories related to the said category/categories of data subject;
- the data recipients or the categories of data recipient;
- data transfers to third countries, where envisaged;
- a general description that allows an assessment beforehand whether the measures adopted to ensure security of the processing are adequate.

6.1.6 Notification fees

The notification fee is EUR 150, plus (if the data controller cannot provide the online notification to be signed with the electronic certified signature) an additional EUR 25 for the paper notification costs.

6.2 Authorisation requirements

Data controllers do not need to obtain authorisation to carry out a data processing activity, except in specific cases provided for by law (ie for data processing of judicial data, sensitive data and for the transfer of personal data to a non-EU member state).

Processing of genetic data, regardless of the entity processing them, shall be allowed exclusively in the cases provided for in ad hoc authorisations granted by the Garante, after having consulted with the Minister for Health who shall seek, to that end, the opinion of the Higher Health Care Council.

Any authorisation procedure is set by law. Authorisations are given by the Garante in general form for certain categories of data processing, only in residual cases are individual authorisations released on express request by the data controller.

6.3 Other registration requirements

Not applicable.

6.4 Register

The Garante holds a public register of notified processing operations which may be consulted by anyone, free of charge, at *https://web.garanteprivacy.it/rgt/NotificaEsplora.php*.

For each processing, the public register contains the same information as is provided in the notification form.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The Code does not contemplate the role of the data protection officer.

7.2 Tasks and powers

Not applicable.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The Code shall not be applied in such a way as to restrict or prohibit the free movement of personal data among EU member states, subject to the taking

of measures under the Code where data are transferred in order to escape application of the provisions.

It is generally prohibited to transfer personal data from the state's territory to countries outside the EU, temporarily or not and in any form and by any means whatsoever, if the laws of the country of destination or transit of the data do not ensure an adequate level of protection of individuals. Account shall also be taken of the methods used for the transfer and the envisaged processing operations, the relevant purposes, nature of the data and security measures. The European Commission has recognised a number of countries as providing for an adequate level of protection.

However, personal data that are the subject of processing may nonetheless be transferred temporarily or not and in any form and by any means from the state's territory to countries outside the EU which do not provide an adequate level of protection, subject to the conditions set out in section 8.2 below.

8.2 Legal basis for international data transfers

Personal data that are the subject of data processing may be transferred from the state's territory to countries outside the EU, temporarily or not and in any form and by any means whatsoever, in the following cases:

- if the data subject has given his/her consent either expressly or, where the transfer concerns sensitive data, in writing;
- if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interests of the data subject;
- if the transfer is necessary for safeguarding a substantial public interest that is referred to by laws or regulations, or else that is specified in the Code where the transfer concerns sensitive or judicial data;
- if the transfer is necessary to safeguard a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right from wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person living together with the data subject or, failing these, the manager of the institution where the data subject is hosted;
- if the transfer is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are transferred exclusively for said purposes and for no longer than is necessary in compliance with the legislation in force applying to business and industrial secrecy;
- if the transfer is carried out in response to a request for access to administrative records or for information contained in a publicly available register, list, record or document, in compliance with the provisions applying to this subject-matter;

- if the transfer is necessary, pursuant to the relevant codes of conduct provided for by the Code, exclusively for scientific or statistical purposes, or else exclusively for historical purposes, in connection with private archives that have been declared to be of considerable historical interest or else in connection with other private archives pursuant to the provisions made in said codes;
- if the processing concerns data relating to legal persons, bodies or associations.

In addition, the Garante can authorise the transfer of personal data to a non-EU member state on the basis of adequate safeguards for data subjects' rights, which can be provided by contractual safeguards or by binding corporate rules. A data subject may enforce his/her rights in the state's territory as set forth by the Code also with regard to non-compliance with the aforementioned safeguards.

8.2.1 Data transfer agreements

The Garante has authorised data transfers on the basis of the European Commission's standard contractual clauses. Where the data transfer is based on these clauses, no individual authorisation must be requested from the Garante. Individual authorisation would however be required where other contractual clauses are used; this authorisation, not common in the Italian system, can be required by the data controller

Recently, the Garante has specifically authorised, with the decision of 27 May 2010, transfers of personal data from the state's territory to countries outside the European Union (from data controller to data processor) made according to a new scheme of standard contractual clauses, containing within itself a provision called 'the subcontracting' according to which the importer (as data processor) can entrust the treatment (or a portion thereof) to a third party (known as 'subcontractors'), also acting as data processor.

8.2.2 Binding corporate rules

The matter of cross-border transfers of personal data has been subject to constant attention during 2010 with respect to the issuance of authorisations to transfer data to third countries in particular on the basis of binding corporate rules (BCRs).

By decisions of 8 April 2010 of 7 October 2010, and of 11 October 2011, the Garante for the first time decided on BCRs developed by important multinational corporate groups and authorised the transfer of data in the manner and for the purpose laid down in the BCRs.

With reference to the BCR, it has to be highlighted that the Garante, with the decisions dated 8 April 2010 and 7 October 2010, ruled for the first time in respect of certain projects of BCRs developed by major multinational corporate groups.

In the first case, in particular, the request for authorisation was submitted by a non-EU multinational group following the conclusion, by the lead authority, of the process of European cooperation under the system of mutual recognition. The request was for intra-group transfers of personal

data relating to employees and customers from the territory of the Italian state, to the subsidiaries based in countries outside the European Union. The Garante, following a complex preliminary investigation, during which it took note of the additional submissions made by the applicant to the Garante (in particular concerning the content and effectiveness of mandatory liability clause and the third beneficiary, and the exact compliance with the security measures prescribed by law), authorised the transfer in accordance with the above procedures laid down in the BCR, for the sole achievement of the purposes stated therein. The Garante has, however, reiterated its power to conduct at any time necessary checks on the legality and propriety of the transfer of data, with regard to all processing operations relating to them, and to adopt, where necessary, blocking or prohibiting decisions. Finally, the Garante stated that the processing operations of personal data, even if carried out after consent is given, will be lawful only where carried out in conformity with existing national legislation and its subsequent amendments, including those relating to protection of personal data, with particular reference to specific provisions on the conditions of legitimacy of the collection data being transferred and on the conditions of legitimacy for the communication of data.

8.2.3 Safe Harbour

There are no specific provisions regarding transfer to countries subject to Safe Harbour.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Confidentiality of personal data is regarded as the fundamental condition of each data processing.

Confidentiality undertakings are, furthermore, contained in the instructions given to persons in charge of processing.

9.2 Security requirements

Personal data undergoing processing shall be kept and controlled in such a way as to minimise, by means of suitable preventative security measures, the risk of their destruction or loss whether by accident or otherwise, and of unauthorised access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Processing personal data by electronic means shall only be allowed if the minimum security measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B of the Code:

- computerised authentication;
- implementation of authentication credentials and management procedures;
- use of an authorisation system;
- regular update of the specifications concerning the scope of the

processing operations that may be performed by the individual entities in charge of managing and/or maintenance of the electronic means;
- protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software;
- implementation of procedures for safekeeping backup copies and restoring data and system availability;
- keeping an up-to-date security policy document;
- implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.

The security requirements of data processing (such as the implementation of the authorisation system, the security policy document and the additional measures applying to processing of sensitive or judicial data) are explained in detail in Annex B of the Code.

The security policy document, which data controllers are obliged to prepare and implement, describes the implementation of all the security measures. Small companies, freelancers and craftsmen processing data exclusively for administrative and accounting purposes are not required to implement this document, for them it is sufficient to make a declaration of conformity of the data processing to the Code signed by a legal representative.

9.3 Data security breach notification obligation

There is no general obligation under Italian law to notify personal data security breaches.

Nevertheless it is, in particular, set out that the provider of a publicly available electronic communications service, where there is a particular risk of a breach of network security, shall inform subscribers and, if possible, users concerning the risk and, when the risk lies outside the scope of the measures to be taken by the provider, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards.

9.4 Data protection impact assessments and audits

There is no general requirement to carry out data protection impact assessments and audits as such under Italian law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

In discharging its tasks, the Garante may request the data controller, the data processor, the data subject or a third party to provide information and produce documents.

The Garante may order that data banks and filing systems be accessed and carry out audits on the spot with regard to premises where the processing takes place or investigations with a view to checking compliance with personal data protection regulations.

10.2 Sanctions

The Code provides for criminal and administrative offences.

Administrative sanctions can in particular be imposed by the Garante for the following offences:

- breach of the provisions on adequate information to data subjects shall be punished by a fine of between EUR 6,000-36,000 (the amount may be increased by up to three times if it is found to be ineffective on account of the offender's economic status);
- assigning data in breach of the provisions of the Code and/or other provisions concerning the processing of personal data shall be punished by a fine of between EUR 10,000-60,000;
- breach of the provision regarding the communication of personal data disclosing health shall be punished by a fine of between EUR 1,000-6,000;
- processing data in breach of the minimum security measures shall be punished with a fine ranging from EUR 10,000-120,000 (with a possible reduction);
- failing to abide by the provisions either setting out necessary measures or laying down prohibitions and administrative sanctions shall be punished with a fine ranging from EUR 30,000-180,000;
- any violation of the right to object shall be punished with a fine ranging from EUR 10,000-120,000;
- breach of the provision on conservation of traffic data shall be punished by a fine of between EUR 10,000-50,000;
- failing to submit on time the notification or providing incomplete information in a notification, in breach of the data controller's duty, shall be punished by a fine of between EUR 20,000-120,000;
- failing to provide the information or produce the documents requested by the Garante shall be punished by a fine of between EUR 10,000-60,000.

Where any of the violations referred to above is less serious having regard to the social and/or business features of the activities in issue, the upper and lower thresholds set forth in the sections can be reduced to two-fifths; in other, more serious cases, in particular if the prejudicial effects produced on one or more data subjects are more substantial or if the violation concerns several data subjects, the upper and lower thresholds of the applicable fines can be doubled.

In the above cases an additional administrative sanction may be applied, consisting of the publication of the injunctive order, in whole or in part, in one or more newspapers as specified in the relevant provision. The offender shall be responsible for the said publication and bear the relevant costs.

The criminal offences include in particular:

- unlawful data processing by any person who, with a view to gaining for himself or another or with intent to cause harm to another, shall be punished, if harm is caused, by imprisonment of between six and 18 months or, if the offence consists of data communication or dissemination, by imprisonment of between one and 24 months

depending on the violation and the seriousness of the offence;
- declaring or attesting to untrue information or circumstances, or else submitting forged records or documents, communications, records, documents or statements that are submitted or made, as the case may be, in a proceeding before the Garante and/or in the course of inquiries, shall be punished by imprisonment of between six months and three years, unless the offence is more serious;
- failing to adopt the minimum security measures in breach of the relevant obligations shall be punished by detention for up to two years.

Furthermore, the conviction of any of the offences referred to in the Code shall entail the publication of the relevant judgment.

10.3 Examples of recent enforcement of data protection rules

From the inspection activity report, it emerges that in 2010 about 474 inspections were carried out and 424 penalty proceedings were initiated, a large number related to providing inadequate information to data subjects, unlawful processing of data, failing to adopt minimum security measures, and breach of the orders of the Garante. The inspections have been particularly focused on the healthcare industry, hotel chains, the activation of multiple phone cards and online training.

There were 55 referrals to the court for criminal violations which concerned, inter alia, the failure to adopt security measures; the falsity of statements and notifications; and the failure to comply with the orders of the Garante. The revenues from the sanctions imposed amounted to a total of about EUR 3,800,000, including EUR 2 million for breaches of disclosure obligations; EUR 800,000 relating to the unlawful processing of data; and EUR 450,000 relating to failure to adopt security measures by private and public companies.

10.4 Judicial remedies

Competence over any disputes concerning the application of the provisions of the Code, including those related either to provisions issued by the Garante with regard to personal data protection or to the failure to adopt such provisions, shall lie with judicial authorities. The relevant proceeding shall be instituted by filing a petition with the clerk's office of the court having jurisdiction over the data controller's place of residence.

The judicial authority shall decide on the case as a single-judge court.

Any petition against an order or decision of the Garante must be filed within 30 days of the date on which said order or decision is communicated or tacitly dismissed. If the petition is filed after that time, the court shall declare that it is inadmissible by an order that may be challenged before the Court of Cassation.

Filing a petition shall not suspend enforcement of the order or decision of the Garante. The court may provide wholly or partly otherwise on serious grounds, after hearing the parties, by issuing an order that may be challenged together with the decision finalising the relevant proceeding.

If there is an imminent danger of serious, irretrievable harm, the court

may take the necessary measures by a reasoned decree, summoning the parties to appear in court in no later than 15 days. During the relevant hearing the court shall uphold, amend or discharge the measures taken by means of said decree.

The judgment may not be appealed, however it may be challenged before the Court of Cassation.

The Garante cannot initiate judicial proceedings.

10.5 Class actions

Class actions in Italy are not permitted with reference data protection.

10.6 Liability

The data controller shall be held liable for any damage as a result of an action in violation of the provisions of the Code. Data subjects that have incurred damage from an action in violation of the Code may thus claim damages from the data controller. The data controller shall be exempt from liability if he proves that he has adopted all adequate measures to avoid the damage.

As far as outsourcing activities are concerned, the data controller and the data processor have liability for the data processing.

In a decision of 5 May 2011 the Garante determined that, in light of the principle of relevant and non-excessive data processing, a website can publish an order for preventive detention but it must be sure to obscure online all non-essential personal information of the person subjected to the precautionary measure (as far as information of a personal nature are not essential to fully represent the legal case), claiming as wrongful the treatment of personal data by the website provider who published the court order in its entirety.

In another decision of 7 July 2011, the Garante declared legitimate the use of satellite tracking of vehicles in relation to the business (in this case, a fleet) for the specific purpose of rendering more efficient the transport service and to quantify correctly the costs to the customer. In light of the above, the Garante stated that only data suitable for tracking the location of vehicles and essential to the compilation of the driving companies' report can be processed.

Latvia

BORENIUS Linda Lejina & Ilze Bukaldere

1. LEGISLATION

1.1 Name/title of the law

The collection and processing of personal data is governed by the Personal Data Protection Law (the Law), adopted by Parliament on 23 March 2000. The legal provisions deriving from the Directive 95/46/EC of the European Parliament and of the Council 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 (the Directive) are incorporated in the Law.

In addition to this, several specific laws also contain provisions on the protection of personal data. For instance, Parliament passed the Biometric Data Processing Law on 21 May 2009 with the aim of ensuring the establishment of unified processing systems of biometric data to determine the identity of a natural person, as well as to prevent the use of alien identity. Likewise, on 13 June 2002, Parliament adopted the Human Genome Research Law in order to regulate the establishment and operation of the single genome database of the population and genetic research, to ensure the voluntary nature and confidentiality of gene donation in respect of the identity of gene donors, as well as to protect persons from the misuse of genetic data and discrimination related to genetic data.

1.2 Pending legislation

There is an intention to adopt a law regarding the Data State Inspectorate (DSI), the state institution supervising the protection of personal data. The initial purpose of such law is to define more precisely the legal status of this institution, the rights and obligations belonging to it and other conditions to enhance the supervision of personal data protection in Latvia.

Since 2010 when the European Commission started to evaluate implementation of the Directive, the DSI is anticipating that in 2012 the European Commission will provide its conclusions and recommendations regarding the evaluation of the normative framework of EU personal data protection, including the status, functions and powers of data protection institutions. Therefore, the DSI is planning to update the respective draft law regarding the DSI within 2012.

1.3 Scope of the law

1.3.1 The main players

- The 'data subject' is a natural person, who may be directly or indirectly identified;
- the 'data controller' is a natural person or a legal person, a state or a

municipality institution, who determines the purposes and the means of processing of personal data, as well being liable for the processing of personal data in accordance with the Law;
- the 'data processor' is a person authorised by a data controller, who carries out personal data processing upon the instructions of the data controller;
- the 'third person' is any natural or legal person, except for a data subject, a data controller or a data processor, who has been directly authorised by a data controller or a data processor.

1.3.2 Types of data

According to the terms defined and used within the Law, 'personal data' are any information related to an identified or identifiable natural person. 'Sensitive data' are personal data, which indicate the race, ethnic origin, religious, philosophical or political convictions, or trade union membership of a person, or provide information as to the health or sexual life of a person. In addition, the Law also defines the identification code of the person as a number that is allocated for the identification of the data subject.

Furthermore, the Law sets forth certain provisions regarding personal data that relate to the commitment of criminal offences, convictions in criminal matters and administrative violation cases, as well as to court adjudications or court case files.

The Law does not provide protection for data related to legal persons. It is explicitly stated within the Law that the purpose of it is to protect fundamental human rights and freedoms of natural persons, in particular the inviolability of private life, regarding the processing of natural persons' personal data. However, it cannot be excluded that the specific rules for personal data protection are indirectly applied to information related to business transactions or legal persons (on the recommendation of the DSI – 'Definition of Personal Data' (2008)). In situations where information on legal persons based on 'substance', 'purpose' or 'result' means that such information also relates to a natural person, it has to be considered to be personal data and the data protection rules are applicable.

The abovementioned recommendation of the DSI also explained that traceable pseudonmyised data are considered to be information relating to an indirectly identifiable person. Actually the use of a pseudonym means that there exists a possibility of identifying a person. According to the DSI recommendation, in such a situation, although the rules of data protection are applicable, the risk of processing such indirectly identifiable information regarding a specific person is low and, therefore, a more flexible application of the rules can be justified than in a case where the processing of information regarding a directly identifiable person is taking place.

With regard to anonymous data, the DSI has explained that the regulation of the Law is not applicable if a data subject is not identifiable. However, the assessment of whether the data permit the identification of an individual and whether such information can be regarded as anonymous, depends on the circumstances of each particular case. In relation to the data of dead

persons, the DSI has interpreted that in principle the information regarding dead persons is not to be regarded as personal data and the rules of the Law are not applicable.

1.3.3 Types of acts/operations

The Law defines personal data 'processing' as any operation carried out regarding personal data, including: data collection; registration; recording; storing; arrangement; transformation; utilisation; transfer; transmission and dissemination; blockage; or erasure. Since the Law does not distinguish between automatic and/or manual data processing, it can be concluded that the regulation of the Law covers both automatic and manual processing of personal data.

1.3.4 Exceptions

The Law does not apply to personal data processing carried out by natural persons for personal or household and family purposes where the personal data collected are not disclosed to third persons. Partial exemptions from the application of the Law exist for certain types of data processing, eg under the Law on Official Secrets.

Furthermore, taking into account the rights of persons to inviolability of private life and freedom of expression, specific provisions of the Law are not applied if personal data are processed for journalistic purposes in accordance with the Law on Press and Other Mass Media, for artistic or literary purposes, and it is not prescribed otherwise by law.

1.3.5 Geographical scope of application

The Law, taking into account the specified exceptions, applies to the processing of all types of personal data, and to any natural or legal person if:

the data controller is registered in the Republic of Latvia;

data processing is performed outside the borders of the Republic of Latvia in territories that belong to the Republic of Latvia in accordance with international agreements; or

the equipment used for the processing of personal data is located in the territory of the Republic of Latvia, except when the equipment is used only for the transmission of personal data through the territory of the Republic of Latvia. In such a case the data controller appoints an authorised person, who is responsible for compliance with the Law.

1.3.6 Particularities

None.

2. DATA PROTECTION AUTHORITY

Data State Inspectorate/*Datu Valsts Inspekcija*
Blaumana street 11/13-15, Riga, LV-1011, Latvia
T: +371 67 22 31 31
F: +371 67 22 35 56
E: info@dvi.gov.lv
W: *www.dvi.gov.lv*

2.1 Role and tasks

The supervision of personal data protection in Latvia is carried out by the DSI, which is subject to the supervision of the Ministry of Justice. The DSI operates independently and permanently by fulfilling the functions specified in regulatory enactments, taking decisions and issuing administrative acts in accordance with the law. The DSI is a state administration institution whose functions, rights and duties are determined by law.

The duties of the DSI in the field of personal data protection are the following:

- to ensure the compliance of personal data processing in Latvia with the requirements of the Law;
- to take decisions and review complaints regarding the protection of personal data;
- to register the personal data processing;
- to propose and carry out activities aimed at raising the effectiveness of personal data protection and provide opinions on the conformity of personal data processing systems to be established by the state and local government institutions to the requirements of regulatory enactments;
- together with the Office of the Director General of the State Archives of Latvia, to decide on the transfer of personal data processing systems to the state archives for storage.

2.2 Powers

In the field of personal data protection, the DSI is entitled:

- in accordance with the procedures prescribed by regulatory enactments, to receive free of charge the necessary information from natural persons and legal persons for the performance of functions pertaining to the DSI;
- to perform an inspection of personal data processing;
- to request data blockage, to request the deletion or destruction of inaccurate or unlawfully obtained data, or to impose a permanent or temporary prohibition on data processing;
- to bring an action in court for violations of the Law;
- to annul the registration certificate for personal data processing if violations are established;
- to impose administrative penalties according to the procedures specified by law regarding violations of personal data processing;
- to perform inspections in order to determine the conformity of personal data processing with the requirements of regulatory enactments.

In order to perform the above duties, the director of the DSI and the DSI employees authorised by the director are entitled:

- to freely enter any non-residential premises where the personal data processing is carried out, and in the presence of the representative of the data controller carry out the necessary inspection or other measures in order to determine the compliance of the personal data processing procedure with the law;
- to require written or verbal explanations from any natural or legal

person involved in personal data processing;
- to require that documents are presented and other information is provided that relates to the personal data processing being inspected;
- to require an inspection of personal data processing, including any equipment or information carrier, and to order an expert's examination to be conducted regarding questions subject to investigation;
- to request assistance from officials of law enforcement institutions or other specialists, if necessary, in order to ensure performance of its duties;
- to prepare and submit materials to law enforcement institutions in order for offenders to be held liable, if necessary;
- to draw up a statement about administrative violations regarding personal data processing.

Officials of the DSI involved in registration and inspections are obliged to ensure that information obtained in the process of registration and inspections is not disclosed, except for the information that is publicly accessible. This prohibition remains in effect after the officials have ceased to fulfil their official duties.

2.3 Priorities

The Annual Report of the DSI for 2009 provided the following priorities for 2010:
- to settle personal data protection questions in relation to the databases of credit recovery and credit history;
- to monitor implementation of data protection requirements for state registries;
- to monitor implementation of data protection requirements in relation to health information;
- to control personal data processing carried out by rights protection institutions;
- to control data protection specialists;
- to prepare a recommendation about the processing of personal data in social networks.

Priorities for 2011 include preparing recommendations regarding the processing of personal data within employment relationships and the protection of children's data in general educational institutions.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

The Law defines the 'consent' of a data subject as a freely, clearly expressed affirmation of will by which the data subject allows his or her personal data to be processed in conformity with information provided by the data controller in accordance with the requirements of the Law.

3.1.2 Form

The Law does not set forth requirements regarding the form of consent of the data subject, except for the processing of sensitive data. Subsequently, the Law explicitly provides that the processing of sensitive data is permitted where a data subject has given his or her written consent for the processing of his or her sensitive data.

Although the Law does not stipulate specific requirements regarding the form of consent (except for sensitive data), the consent of a data subject serves as a legal basis for personal data processing; therefore, it may be necessary for a data controller to arrange and by whatever means solidify that a particular data subject has provided his or her consent to particular data processing activities. This may be helpful to establish that a data controller has provided a data subject with all information as requested by the Law and to determine the scope of personal data processing and/or other applicable terms and conditions.

3.1.3 In an employment relationship

With regard to the processing of sensitive data, which is prohibited by the Law, an exception exists whereby such data may be processed without the consent of the data subject if it is provided for by regulatory enactments, which regulate legal relations regarding employment, and such regulatory enactments guarantee the protection of personal data.

So far the DSI has not published its opinion or interpretation regarding the validity of employee consent. Within the Public Annual Report 2008, the DSI provided its commentaries regarding the requesting of passport copies within an employment relationship. The DSI has pointed out that the employer has the right to obtain the passport copy only in those cases when the employee has expressed his consent freely and clearly to submitting the passport copy to the employer. Nevertheless, the DSI has not interpreted or provided any opinion regarding the validity of employee consent.

3.2 Other legal grounds for data processing

According to the Law, personal data processing is permitted only if not prescribed otherwise by law, and at least one of the following conditions exists:

- the personal data processing derives from contractual obligations of the data subject or, taking into account a request from the data subject, the processing of data is necessary in order to conclude the relevant contract;
- the data processing is necessary for the data controller to perform his duties as specified by law;
- the data processing is necessary to protect vitally important interests of the data subject, including life and health;
- the data processing is necessary in order to ensure that the public interest is complied with or to fulfil functions of public authority for the performance of which the personal data have been transferred to the data controller or transmitted to a third person;

- the data processing is necessary in order to comply with the fundamental human rights and freedoms of the data subject, exercise the lawful interests of the data controller or of such third person to whom the personal data have been disclosed.

The Law also sets forth legal grounds for sensitive data processing, that is prohibited except in cases where:

- the data subject has given his or her written consent for the processing of his or her sensitive data;
- special processing of personal data, without requesting the consent of the data subject, is provided for by regulatory enactments, which regulate legal relations regarding employment, and such regulatory enactments guarantee the protection of personal data;
- personal data processing is necessary to achieve the lawful, non-commercial objectives of non-governmental organisations and their associations, if such data processing is only related to the members of these organisations or their associations and the personal data are not transferred to third parties;
- personal data processing is necessary for the purposes of medical treatment, the provision or the administration of health care services and the distribution or the administration of medicine and medical devices;
- the processing concerns such personal data as are necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings;
- personal data processing is necessary for the provision of social assistance and it is performed by the provider of social assistance services;
- personal data processing is necessary for the establishment of Latvian National Archive foundation and it is performed by the State Archives and institutions with state storage rights approved by the Director-General of the State Archives;
- personal data processing is necessary for statistical research that is carried out by the Central Statistics Bureau;
- the processing relates to such personal data that the data subject has him or herself made public;
- personal data processing is necessary for the performance of state administration functions or for the development of the state information systems determined by the law;
- personal data processing is necessary for the natural or legal person's rights or legitimate interests, when requiring compensation according to the insurance contract;
- medical data about a patient are processed within research according to the Patients Rights Law.

Furthermore, the Law stipulates the legal basis for processing of personal identification (classification) codes. Such may be processed in one of the following cases:

- the consent of the data subject has been received;

- the processing of the identification codes arises from the purpose of the personal data processing;
- the processing of the identification codes is necessary to ensure the continuing anonymity of the data subject;
- a written permit has been received from the DSI.

3.3 Direct marketing and cookies

The Law does not explicitly regulate direct marketing activities, however, it sets out that a data subject has the right to prohibit the processing of his or her personal data for commercial purposes. The Law on Information Society Services provides for the prohibition on sending commercial communications, namely, it is prohibited to use for sending a commercial communication the system of automatic calling (terminal), which operates without the involvement of a person (automatic calling devices), electronic mail or fax devices (facsimiles), unless the recipient has provided free and unambiguous consent in advance.

The Law on Information Society Services establishes that a service provider, who has obtained email addresses within its commercial transactions from service receivers, is entitled to use them for other commercial communications if:

- the commercial communications are sent regarding similar goods or services to the service provider;
- the recipient has not already initially rejected the further use of its email address;
- each time a commercial communication is sent, the recipient is provided with the clear and free of charge possibility (by submitting an application or by sending an announcement electronically) to refuse the further use of its email address.

Other kinds of communication using publically accessible electronic communication services may take place if a recipient has provided in advance his free and unambiguous consent.

With regard to cookies and the implementation of Article 5(3) of the ePrivacy Directive, as amended by Directive 2009/136/EC, the provisions of the Law on Information Society Services regarding the storage of information in terminal equipment apply. It is stipulated that the storage of information within the terminal equipment of a subscriber or a user or access to the information stored in the terminal equipment is permitted if the subscriber or user has provided his/her consent after receiving clear and comprehensive information regarding the aim of abovementioned processing in accordance with the Law. Such consent is not necessary if the storage of information within the terminal equipment or the access to the information stored in the terminal equipment is necessary to ensure the circulation of information within the electronic communications network, or for the intermediary service provider in order to provide the service requested by a subscriber or a user.

3.4 Data quality requirements

In order to protect the interests of a data subject, a data controller is obliged to ensure that the personal data are processed fairly, lawfully and only in conformity with the intended purpose and to the extent required. Besides, a data controller has to ensure that personal data are stored so that the data subject is identifiable for a relevant period of time, which does not exceed the time period prescribed for the intended purpose of the data processing. Likewise, a data controller has to ensure the accuracy of personal data and their timely update, rectification and deletion, if personal data are incomplete or inaccurate in accordance with the purpose of the personal data processing.

3.5 Outsourcing

The Law provides for the possibility that a data controller may entrust personal data processing to the data processor by concluding a written agreement. The data processor may process personal data entrusted to him or her only within the scope determined in the agreement and in conformity with the purposes provided for in it and in accordance with the instructions of the data controller, if they are not in conflict with regulatory enactments. Prior to commencing the personal data processing, the data processor is obliged to carry out security measures determined by the data controller for the protection of the system in accordance with the requirements of the Law.

3.6 Email, internet and video monitoring

3.6.1 General rules

In 2009, the DSI adopted the recommendation 'Data Processing by Video Monitoring' and concluded that in most situations, video monitoring counts as processing of personal data and the images acquired as a result of video monitoring contain personal data the processing of which has to be performed in accordance with the Law. Thus, the particular recommendation of the DSI is applicable to video monitoring which results in images or other data of identifiable persons being acquired. According to the DSI, the primary reason when deciding on the necessity to perform video monitoring is the existing problem and the objective to be achieved from video monitoring in order to solve the existing problem. Thus, a data controller may start the video monitoring only when he has established that the video monitoring is necessary, namely, the benefits of video monitoring will be greater than the threat of privacy caused to a person, and that he/she will ensure that the intended objective is achieved in a manner which least violates the privacy rights of a person. In addition to other conditions to be observed, a data controller is obliged to inform persons when video monitoring is taking place.

With regard to email and internet monitoring, the Law does not provide specific and explicit regulation on this. However, email and internet monitoring, as with any personal data processing, is permitted if there exists a legal basis as provided by the Law, whereas the processing of sensitive data

is prohibited, except in situations set forth under the Law. Otherwise, all other rules of personal data processing are applicable.

3.6.2 Employment relationship

With regard to the video monitoring of employees, it is stated within the DSI recommendation that the Law also applies to natural persons as employees and an employee is entitled to the inviolability of private life in the work place. Therefore, it is necessary to ensure the proportionality between the rights of employees and the interests of the employer. Therefore, the video monitoring of employees is permissible in exceptional situations, but never in the toilets and rest rooms of a work place.

With regard to email and internet monitoring in an employment relationship, as noted above, the Law does not include specific and explicit regulation on such matters. However, taking into account the purpose of the Law to protect the fundamental human rights and freedoms of natural persons, it is necessary to ensure proportionality between the rights of employees and the interests of the employer. Nevertheless, it can be concluded that the rules on personal data processing are applicable and it is important that employees are informed about the rules on the use of employer's email and/or internet access, including the possibility that their activities may be monitored by an employer.

4. INFORMATION OBLIGATIONS

4.1 Who

When processing personal data, the general responsibility to provide information is to be assumed by the data controller. When acquiring personal data, regardless whether from a data subject or otherwise, a data controller is obliged to provide the data subject with certain information. A data controller is obliged to disclose personal data in cases provided for by the Law to officials of state and municipal institutions.

4.2 What

The information to be provided by a datacontroller to a data subject depends on whether the personal data are acquired from a data subject or not. Thus, a controller has a duty to provide a data subject with the title or name and surname, and the address of the data controller and the data processor and the intended purpose and legal basis for the personal data processing. As follows, based on the request from a data subject, a data controller has a duty to provide the data subject with information on:

- the possible recipients of the personal data;
- the right of a data subject to gain access to his or her personal data and to make corrections to such data;
- whether providing an answer is mandatory or voluntary, as well as the possible consequences of failing to provide an answer;
- the personal data categories and the source of the data.

As for the obligation of the data controller to disclose personal data to officials of state and municipal institutions, the personal data to be disclosed

by a data controller are to be determined by laws providing the legal basis for such a request.

4.3 Exceptions

When collecting personal data from a data subject, a data controller has no duty to provide a data subject with the specified information if carrying out personal data processing without disclosing its purpose is authorised by law.

Furthermore, if the personal data have not been obtained from a data subject, a data controller has no duty to provide information to a data subject, if:

- the law provides for the processing of personal data without informing the data subject of it;
- when processing personal data for scientific, historical or statistical research, or the establishment of Latvian National Archive foundation, or when informing the data subject requires disproportionate effort or is impossible.

4.4 When

The information has to be provided by the data controller to a data subject when the personal data are acquired from the data subject or, if personal data have not been obtained from a data subject, when collecting or disclosing such personal data to a third person for the first time.

4.5 How

The Law does not set forth specific rules as to the form and how the information has to be provided by a data controller to a data subject. Nevertheless, it can be concluded that a data controller has to provide the information as requested by law in the form and manner acceptable to a data subject.

For example, when obtaining personal data from a data subject, a data controller has to evaluate the particular situation and to provide the necessary information to a data subject in a form and manner enabling a data subject to properly receive and process such information without unnecessary burden. Furthermore, considering that it is the duty of data controller, it may be helpful for a data controller to ensure and maintain certain evidence that such information was provided to the data subject.

As for requests from officials of the state and local government institutions, personal data may be disclosed based on a written request or agreement, indicating the purpose for the use of the data, if not prescribed otherwise by law. In the request for personal data, information shall be provided that allows identification of the personal data requester and the data subject, as well as the scope of the personal data requested.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

In addition to the rights referred to above regarding the information to be provided to a data subject, a data subject also has the right to obtain all

the personal data that have been collected concerning him or her in any personal data processing system. Furthermore, a data subject has the right to obtain the information concerning those natural or legal persons who, within a prescribed time period, have received information from a data controller concerning the data subject.

A data subject also has the right to request the following information:

- the title or name, surname, and address of the data controller;
- the purpose, scope and method of the personal data processing;
- the date when the personal data concerning the data subject were last rectified, deleted or blocked;
- the source from which the personal data were obtained unless the disclosure of such information is prohibited by law;
- the processing methods used by the automated processing systems that take individual automated decisions (see section 5.6 below).

5.1.2 Exceptions

The rights of a data subject to access all the personal data collected concerning him or her are subject to limitations where the disclosure of such information is prohibited by law due to national security, defence and criminal law, or for the purpose of ensuring the financial interests of the state in tax collection matters. Furthermore, it is prohibited to provide to a data subject information on particular state institutions that administer criminal procedures, carry out investigative field work, or other institutions provided by law that have requested information on the data subject.

5.1.3 Deadline

A data subject has the right, within a period of one month from the date of submission of the relevant request (not more than two times a year), to receive such information in writing.

5.1.4 Charges

A data subject has the right to receive such information free of charge.

5.2 Rectification

5.2.1 Right

A data subject has the right to request that his or her personal data are supplemented or rectified if the personal data are incomplete, outdated, false, unlawfully processed or are no longer necessary for the purposes for which they were collected.

5.2.2 Exceptions

Rectification is not applicable if the processed data are used only for the needs of scientific and statistical research or the establishment of Latvian National Archive foundations in accordance with and based on regulatory enactments and no activities are carried out and no decisions are taken regarding the data subject.

5.2.3 Deadline
A data subject has the right to receive from a data controller a written reasoned answer regarding the request within one month from when the request was submitted.

5.2.4 Charges
The Law does not provide that any charge should be applicable in cases when a data subject exercises his/her rights to rectify the personal data collected and processed.

5.3 Erasure
5.3.1 Right
A data subject has the right to request that his or her personal data are destroyed if the personal data are incomplete, outdated, false, unlawfully processed or are no longer necessary for the purposes for which they were collected.

5.3.2 Exceptions
Erasure is not applicable if the processed data are used only for the needs of scientific and statistical research or the establishment of Latvian National Archive foundations in accordance with and based on regulatory enactments and no activities are carried out and no decisions are taken regarding the data subject.

5.3.3 Deadline
A data subject has the right to receive from a data controller a written reasoned answer regarding the request within one month from when the request was submitted.

5.3.4 Charges
The Law does not provide that any charge should be applicable in cases when a data subject exercises his/her rights to erase the personal data collected and processed.

5.4 Blocking
5.4.1 Right
A data subject has the right to request that the processing of his or her personal data is suspended, if the personal data are incomplete, outdated, false, unlawfully processed or are no longer necessary for the purposes for which they were collected.

5.4.2 Exceptions
Blocking is not applicable if the processed data are used only for the needs of scientific and statistical research or the establishment of Latvian National Archive foundations in accordance with and based on regulatory enactments and no activities are carried out and no decisions are taken regarding the data subject.

5.4.3 Deadline

A data subject has the right to receive from a data controller a written reasoned answer regarding the request within one month from when the request was submitted.

5.4.4 Charges

The Law does not provide that any charge should be applicable in cases when a data subject exercises his/her rights to block the personal data collected and processed.

5.5 Objection

5.5.1 Right

If the data subject is able to justify that the personal data are incomplete, outdated, false, unlawfully obtained or no longer necessary for the purposes for which they were collected, the data controller has an obligation to rectify this inaccuracy or violation without delay and notify third parties who have previously received such personal data.

5.5.2 Exceptions

Objection is not applicable if the processed data are used only for the needs of scientific and statistical research or the establishment of Latvian National Archive foundations in accordance with and based on regulatory enactments and no activities are carried out and no decisions are taken regarding the data subject.

5.5.3 Deadline

A data subject has the right to receive from a data controller a written reasoned answer regarding the request within one month from when the request was submitted.

5.5.4 Charges

The Law does not provide that any charge should be applicable in cases when a data subject exercises his/her rights to object to the personal data collected and processed.

5.6 Automated individual decisions

5.6.1 Right

A controller has a duty to review an individual decision that has been taken only based on automated data processing, and creates, amends, determines or terminates legal relations if a data subject disputes such a decision.

5.6.2 Exceptions

A data controller may refuse to review an automated individual decision if it has been taken based on the law or based on the contract that has been concluded with the data subject.

5.6.3 Deadline

The Law does not set forth explicit rules on the deadline regarding an automated individual decision.

5.6.4 Charges

The Law does not provide that any charge should be applicable in cases when a data subject exercises his/her right to have an automated individual decision reviewed.

5.7 Other rights

5.7.1 Right

A data subject has the right to prohibit the processing of his/her personal data:

- for commercial purposes;
- where the data processing is necessary to exercise the lawful interests of the data controller or of such third person to whom the personal data have been disclosed, complying with the fundamental human rights and freedoms of the data subject;
- for their use regarding information society services;
- for their use within the market and public opinion research or genealogical research.

Furthermore, if a data controller fails to respect the obligations determined in the Law, a data subject has the right to appeal to the DSI regarding the refusal of a data controller to provide the information referred to or perform the activities referred to in the Law. To the appeal statement to the DSI, a data subject must attach the documents to prove that a data controller refuses or fails to perform the obligations determined by the Law.

5.7.2 Exceptions

The rights to prohibit the processing of personal data are restricted in cases where the law provides otherwise.

5.7.3 Deadline

The Law does not set forth explicit rules on the deadline regarding such rights of a data subject to prohibit specific personal data activities or to appeal to the DSI.

5.7.4 Charges

The Law does not provide that any charge should be applicable in cases where a data subject exercises his/her rights to prohibit specific personal data activities or to appeal to the DSI.

6. REGISTRATION OBLIGATIONS

On 1 July 2009, amendments to the Law became effective implementing changes to the procedure for the registration of data processing. These amendments specify the registration procedure by setting out additional exceptions where it is not necessary to register personal data processing with the DSI.

6.1 Notification requirements

6.1.1 Who

All state and local government institutions, and natural persons and legal persons that carry out or wish to commence personal data processing, are obliged to register it.

6.1.2 What

Before 2007, data controllers were required to register systems for personal data processing. According to current law, data controllers are required to register the processing of personal data.

6.1.3 Exceptions

The registration procedure is not applicable to personal data processing:
for the purposes of bookkeeping and personnel record keeping;

- for the information systems of state and local government institutions when the data gathered there are publically available;
- for journalistic purposes in accordance with the Law on Press and Other Mass Media;
- for archiving purposes in accordance with the Law on Archives;
- if it is carried out by religious organisations;
- if the data controller has registered the personal data protection officer in accordance with the procedures prescribed in the Law;
- if data processing is carried out when there is consent from a data subject, the personal data processing derives from contractual obligations of the data subject or, taking into account a request from the data subject, the processing of data is necessary in order to conclude the relevant contract or personal identification (classification) codes are processed in cases provided by the Law;
- it is carried out for scientific, statistical and genealogical research purposes.

The above exemptions from the duty to register the personal data processing with the DSI are not applicable if:

- the personal data will be transferred to a country that is not a member state of the European Union or the European Economic Area (EEA);
- the personal data are processed in relation to the provision of financial services, market or public opinion research, selection or evaluation of personnel as entrepreneurship if it is provided as a service to other companies, state institutions, natural persons, raffles or lotteries;
- information on a person's health is processed;
- personal data processing relates to criminal offences or criminal records in criminal and administrative violation cases.

6.1.4 When

The Law provides that a person who wishes to commence personal data processing, is obliged to submit a registration application to the DSI. Therefore a controller has to comply with the registration obligation before the processing of personal data is started.

Likewise, before making changes to the personal data processing, a data controller has to notify such changes to the DSI, except for the information regarding the technical and organisational measures to ensure the protection of the personal data. If technical and organisational measures have been changed so that they significantly affect the protection of the personal data, the information has to be submitted to the DSI within a period of one year.

Furthermore, if a data controller changes or operations of a data controller are terminated, he or she submits to the DSI the application to exclude the personal data processing from the register.

6.1.5 How

The persons who wish to commence the processing of personal data, submit a registration application in Latvian to the DSI that includes the following information:

- the name, surname and personal code (for a legal person – the title and the registration number), address and telephone number of the data controller;
- the name, surname, and personal code of the personal data processor (if applicable), address and telephone number (for legal persons – the title and the registration number);
- the legal basis for the personal data processing;
- the types of personal data and the purposes of personal data processing;
- the categories of data subjects;
- the categories of personal data recipients;
- the intended method of personal data processing;
- the foreseen method to obtain personal data;
- the place of personal data processing; and
- the holder of information resources or technical resources, as well as the person responsible for the information system security and technical and organisational measures ensuring the protection of personal data.

The Cabinet of Ministers (the government) has adopted standard samples for the application form on: (i) the registration of personal data processing; (ii) the notification of the changes regarding the personal data processing; and (iii) the exclusion of the personal data processing from the register of the personal data processing. These forms are available at: *www.dvi.gov.lv/fpda/*.

Furthermore, when receiving an application to register personal data processing, the DSI identifies the personal data processing where the risks related to the rights and freedoms of the data subject are possible and determines the pre-registration checking (please see also section 6.3 for more on pre-registration checking) required for such processing. When registering the personal data processing, the DSI issues a certificate of personal data processing registration to the data controller or to his or her authorised person.

Information on the activity of the DSI can be found in its Annual Report. For example, in the Annual Report for 2009 it stated that in that year the DSI registered 384 processings of personal data and 93 changes to the processing of personal data. In 2009, the particular spheres of risk to data processing were determined to be: the credit information of a data subject;

the health and sexual life of a data subject; criminal or unlawful offences; and processing wherein the personal data are transferred to countries outside the EU. In accordance with these determined spheres of risk, the DSI carried out 157 pre-registration inspections. Also in 2009 the DSI took 174 decisions to exclude the processing of personal data from the registry.

6.1.6 Notification fees

The state fee for the registration of personal data processing with the DSI is LVL 40.00. Where a controller is a natural person or a small company corresponding to the definition included in Annex 1 to Commission Regulation No 364/2004 (amending Regulation No 70/2001 with regard to the extension of its scope to include aid for research and development), then the state fee for the registration of personal data processing is LVL 20.00.

The state fee for the registration of changes to personal data processing with the DSI is LVL 20.00. Where a controller is a natural person or a small company corresponding to the definition included in Annex 1 to Commission Regulation No 364/2004 (amending Regulation No 70/2001 with regard to the extension of its scope to include aid for research and development), then the state fee for the registration of changes to the personal data processing is LVL 10.00.

The applicable state fee must be paid before submitting an application to the DSI either by transferring the amount to the specified bank account of the State Treasury or using a payment card at the DSI. State and municipality institutions are exempted from paying the state fee.

6.2 Authorisation requirements

Data controllers do not need to obtain authorisation to carry out a data processing activity, however, authorisation is required for data protection officers. Authorisation may be required for the transfer of personal data to a country which does not provide an adequate level of protection.

The Law does not prescribe in detail the authorisation procedure needed to acquire permission for the transfer of personal data. The evaluation of the level of personal data protection and the issuing of permission in writing for the transfer of personal data can be requested from the DSI along with other possibilities to transfer personal data abroad. Within the DSI recommendation 'Transfer of Personal Data to Other Countries', it is explained that in such situations the DSI performs an evaluation of the level of personal data protection if other conditions, which permit the personal data transfer without the existence of an adequate level of data protection, are not applicable. Before providing its consent for the transfer of personal data, the DSI ascertains that there exist no other appropriate conditions for the transfer of personal data abroad. Within the noted recommendation, the DSI points out that where it consents to such transfer of personal data, then the DSI has to inform the European Commission and data protection institutions of other member states. Therefore, if a person desires to obtain such consent from the DSI, it recommends consulting them before sending them the respective application/request.

6.3 Other registration requirements

Pre-registration checking (that is, checking, which is performed after a data controller has submitted to the DSI the application to register the personal data processing) is carried out according to areas of risk as set forth by the DSI. Such areas of risks are reassessed yearly. For example, in 2009 the DSI set forth that the areas of risk in the processing of personal data were: credit information of a data subject; information regarding health and sexual life of person; information regarding criminal or illegal offences of person; and the processing of personal data, wherein such data are transferred to third countries outside the EU.

The DSI carries out the pre-registration checking by evaluating the submitted application to register the personal data processing. Where a data controller is planning to process personal data in the areas of risk, the DSI can require provision of internal security regulations, conclusions of audits and other documents, which regulate the methods of processing and protection of personal data and reflect the scope of personal data processing and the compliance with data security within a data controller's company or institution. Such documents are requested in addition to the initial application to register the personal data processing in order to evaluate the conformity of personal data processing with the requirements of the law. In individual situations the conformity of provided information is examined by performing inspections at the place(s) where personal data are processed.

The Law does not provide other activities or subjects to be registered with the DSI in order to ensure the protection of personal data.

6.4 Register

The Law provides that the DSI has to maintain the Register of Personal Data Processing and the Register of Personal Data Protection Officers. The information specified by the Law is indicated in these registers and they are publicly available *www.dvi.gov.lv/registri*. Both registers are the component parts of the personal data processing supervision information system. The personal data processing supervision information system is the state information system and its operations are organised and administered by the DSI.

7. DATA PROTECTION OFFICER

As stated in the DSI Annual Report for 2009, since 2007 the DSI has implemented an alternative to the registration of personal data processing, by overseeing the establishment of an institute of personal data protection officers. Registration of a personal data protection officer with the DSI is an alternative to the registration of personal data processing, namely, data controllers who register data protection officers with the DSI, are entitled not to register the processing of data.

In 2009 the DSI organised four examinations of data protection officers, and overall 47 persons were tested. In the same year, the DSI certified 17 specialists to be data protection officers.

7.1 Function recognised by law

Personal data protection officers organise, control and supervise compliance with personal data processing carried out by a data controller within the requirements of the Law. According to the requirements of the Law, a data protection officer has to have higher education in jurisprudence, information technology or a similar field and has to be trained according to the order specified by the Cabinet of Ministers. A data controller grants the necessary tools to the personal data protection officer and provides the information necessary to perform the data protection officer's tasks.

7.2 Tasks and powers

A personal data protection officer must create a register containing similar information as required to be provided to the DSI when registering the processing of personal data. Such information has to be provided free of charge by a personal data protection officer upon the request of a data subject or the DSI. The obligation of the personal data protection officer is to retain and not disclose without legal grounds, personal data even after termination of the employment relationship or resigning from office. A personal data protection officer has to prepare an annual report on his or her activities to submit it to the data controller.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

According to the provisions of the Law, personal data may be transferred to another country that is not a member state of the EU or the EEA, if that country ensures a level of data protection that corresponds to the relevant level of protection in force in Latvia. Exemptions from compliance with this requirement are permissible if a controller undertakes to perform the supervision of the performance of the relevant protection measures and at least one of the following conditions is complied with:

- the data subject has given consent;
- the transfer of the data is necessary in order to fulfil an agreement between a data subject and a data controller; the personal data are required to be transferred in accordance with contractual obligations binding upon a data subject or taking into account a request from a data subject; or the transfer of data is necessary in order to enter into a contract;
- the transfer of the data is necessary and requested pursuant to the prescribed procedures, in accordance with significant state or public interests, or is required for legal proceedings;
- the transfer of the data is necessary to protect the life and health of a data subject;
- the transfer of data concerns such personal data that are public or have been stored in a publicly accessible register.

Notwithstanding the above, there exists a possibility for the DSI to perform an evaluation of the level of personal data protection and provide its written approval to transfer the data to the specified country, in specified

circumstances, and for a specified company/institution. Please see comments regarding the authorisation of DSI provided for the transfer of personal data for the transfer of the personal data in section 6.2.

8.2 Legal basis for international data transfers

8.2.1 Data transfers agreements

As noted in the Recommendation of the DSI on 'transfer of personal data to other countries' of 2009, there exist different types of agreements, which can be used to transfer personal data outside the EEA. Such agreements can either be agreements which are drafted taking into account the standard contractual clauses approved by the European Commission, or other agreements ensuring an adequate level of personal data protection. The DSI does not provide its consent to transfer personal data to third countries, if such transfer is carried out on the basis of mutually concluded agreements, and the DSI is not providing any kind of approval to such agreements. In other words, personal data may be transferred on the basis of such agreements without the need to obtain authorisation (notification is still required, though).

The Law stipulates that in order for a data controller to ensure the supervision of the performance of the relevant protection measures as requested, a controller and a personal data receiver have to conclude an agreement on the transfer of personal data.

On 16 August 2011 the Cabinet of Ministers adopted the regulation No 634 on the mandatory terms and conditions to be set forth within agreements on data transfers (the Regulation). The Regulation stipulates the mandatory terms and conditions to be set forth within an agreement on data transfers to countries which are not member states of the EU or the EEA and which do not ensure a level of protection which corresponds to the relevant level of protection that is in force in Latvia. Consequently, the Regulation sets forth provisions, which are to be included in such agreement both regarding the obligations of a data controller and a data receiver and regarding the mandatory technical and organisational requirements for personal data protection. In addition, this Regulation sets forth that such agreement may be concluded as a separate agreement, or the terms and conditions of it may be included in another agreement and that the text of the agreement is to be translated into Latvian or into several languages, one of which is Latvian.

The Regulation also includes provisions which provide that disputes regarding non-compliance with the agreement are reviewed by a court of the Republic of Latvia in accordance with laws applicable within the territory of the Republic of Latvia. Within the annotation of the Regulation it is explained that since it is necessary to ensure the same personal data protection in another country as there is in Latvia, any disputes which result from an agreement are to be settled by a court of the Republic of Latvia, in order to ensure the application of corresponding requirements of personal data protection.

Likewise, it is set forth that the DSI publishes a sample agreement on its homepage *www.dvi.gov.lv*. It has to be noted that this Regulation provides

the transition period until 1 May 2014; until that time a controller has to ensure that agreement concluded before the enactment day of this Regulation complies with the requirements of the Regulation.

8.2.2 Binding corporate rules

As it is explained in the Recommendation of the DSI on 'transfer of personal data to other countries' of 2009, binding corporate rules can be approved in the form of internal contracts, agreements, policies or procedures, and such rules must ensure the necessary protection within a group of companies. In order to use such rules for free data processing (transfer) within a group, they must be approved by all respective data protection institutions in the EU, which cooperate with each other when providing such approval and verify that such rules do correspond. Latvia takes part in the mutual recognition procedure. The DSI provides its approval for the use of such rules within Latvia taking into account specific provisions of the Law and the Directive. As regards the specific provisions of Law, please see section 6.2. At the same time, if the binding corporate rules are used by a subsidiary established by a foreign company for the processing of personal data carried out within Latvia, than the foreign company as a controller is obliged to appoint the authorised person, who is responsible for the compliance with the Law, at the same time a controller is obliged to perform the registration of personal data processing as required by the Law.

8.2.3 Safe Harbour

Within the above recommendation of the DSI, it provides that there is no need for authorisation where personal data are transferred to an organisation that is certified under the US Safe Harbour scheme.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Natural persons involved in personal data processing are obliged to make a commitment in writing to preserve and not to disclose the personal data in an unlawful manner. Such persons have a duty not to disclose the personal data even after termination of the legal employment relationships or other contractually specified relations. Also the obligation of the personal data protection officer is to retain and not to disclose without legal grounds the personal data even after termination of the employment relationship or resigning from office. Furthermore, the officials of the DSI involved in registration and inspections are obliged to ensure that the information obtained during the process of registration and inspections is not disclosed, except for the information that is publicly accessible. Also, with respect to DSI officials, such prohibition remains in effect after the officials have ceased to fulfil their official duties.

9.2 Security requirements

The Law provides that the mandatory technical and organisational requirements for the protection of personal data processing are determined

by the Cabinet of Ministers. On 30 January 2001, the Cabinet of Ministers passed its Regulation No 40 on 'obligatory technical and organisational requirements for protection of personal data processing systems'.

Obligatory technical protection of personal data is carried out using physical and logical protection against threats to personal data caused by physical impact and the protection which is realised with software, passwords, cryptography and other logical protection means. Additionally, when carrying out personal data processing a data controller has to provide:

- access to technical resources which are used for personal data processing and protection (including personal data) only by authorised persons;
- that registration, transfer, arrangement, modification, transmission, copying and other processing of information carriers where personal data are saved is carried out only by exclusively authorised persons;
- that personal data collection, saving, arrangement of saved personal data, storing, copying modification, correction, deleting, elimination, archiving, reserve copying and blocking is provided only by authorised persons, as well as the possibility to track down personal data, which were processed without authorisation, the processing time and person who processed personal data;
- that technical resources used for the personal data processing is moved only by authorised persons;
- that when transferring personal data the information on the time of transfer; the person who transferred the data; the person who received the data; and personal data which are transferred, is maintained;
- that when receiving personal data, the information on the time of receipt; the person who handed over the data; the person who received the data and the personal data which have been received, is maintained.

A data controller, when processing personal data, has to prepare internal data protection regulations, which establish:

- persons responsible for the information resources, technical resources and personal data protection, their rights and obligations;
- personal data protection classification by its value and degree of confidentiality;
- technical resources, by which personal data processing is provided;
- organisational procedure of personal data processing, establishing personal data processing time, place and order;
- activities which should be carried out for protection of technical resources in cases of emergency (fire, flood);
- means with which protection of technical resources is provided against intentional damage and illegal acquisition;
- order of storing and elimination of data carriers;
- length of passwords and conditions on its structure (minimal length of password is eight symbols);
- regulations on password use, as well as period of time after which password should be changed;
- action if password or cryptography key is becomes known to other persons;
- rights, obligations, limitation and liability of users of personal data.

A data controller carries out each year an interior audit of personal data processing and prepares an overview of activities, which were performed in the sphere of information protection. Besides, a data controller informs persons, who process the personal data, about obligatory technical and managerial requirements for the protection of personal data processing.

9.3 Data security breach notification obligation

The Law does not establish an obligation on a data controller to notify a data subject or the DSI of any breach of the rules regarding the processing of personal data. However, the Law on Information Society Services notes that the DSI, within its competence, is one of the supervisory institutions under this law. The law imposes an obligation on an intermediary service provider (a provider of the information society service, which ensures the transmission of information in an electronic communication network, access to an electronic communication network or the storage of information) to immediately inform supervisory institutions about possible violations of the law by a service recipient.

9.4 Data protection impact assessment and audits

9.4.1 Who

According to the Law, state and local government institutions are required to carry out and submit to the DSI audit reports on personal data processing.

9.4.2 What

The audit reports on personal data processing have to include a risk analysis and a report regarding measures implemented in the field of the information security. More detailed requirements on personal data processing by state and local government institutions are set out in Regulation 1322 of the Cabinet of Ministers. As well as other more detailed requirements, within the risk analysis it is necessary to point out the risk factors influencing the processing of personal data in accordance with the established risks for each purpose of personal data processing separately. Likewise, a compliance assessment has to be prepared for each purpose of personal data processing separately. Furthermore, an auditor has to provide reasoned conclusions and suggestions on the established facts.

9.4.3 When

The Law and the above regulation of the Cabinet of Ministers set forth that an audit regarding the processing of personal data must be carried out once every two years.

9.4.4 How

With regard to the compliance assessment, the above-noted regulation of the Cabinet of Ministers includes a sample form as an appendix. On this form, issues to be assessed are listed along with the assessment possibilities using 'yes', 'no' or 'partly', including the instructions to provide conclusions, prioritised suggestions, the person responsible for implementing such suggestions and the

date of implementation of the suggestion (such commentaries must be provided if the particular issue is assessed as 'no' or 'partly').

The sample form sets forth the following main issues to be assessed, and each main issue is subdivided into several related specified matters and questions:

- the processing of personal data in compliance with the foreseen purposes and only in compliance with them;
- the correctness of personal data;
- the storage of personal data;
- the processing of personal data in compliance with the rights of a data subject;
- the security of personal data;
- the transfer of personal data to another country, which is not a member state of the EU or the EEA;
- the use of services of a personal data processor;
- the registration of personal data processing; and
- the implementation of suggestion of the internal audit on the processing of personal data.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

As already noted above, in the field of personal data protection to perform the duties set forth by the Law, the DSI is entitled:

- to freely enter any non-residential premises where personal data processing is carried out, and in the presence of the representative of the data controller carry out the necessary inspection or other measures in order to determine the compliance of the personal data process with the law;
- to require written or verbal explanations from any natural or legal person involved in personal data processing;
- to require that documents are presented and other information is provided which relates to the personal data process being inspected;
- to require inspection of a personal data processing, any equipment or information carrier of personal data, and to determine an expert's examination to be conducted regarding questions subject to investigation;
- to request assistance from officials of law enforcement institutions or other specialists, if necessary, in order to ensure performance of its duties;
- to prepare and submit materials to law enforcement institutions in order for offenders to be held liable, if necessary;
- to draw up a statement regarding administrative violations regarding the personal data processing.

With regard to administrative liability, the Administrative Violations Code provides that the DSI is entitled to examine particular administrative violation matters regarding the processing of personal data and to impose the relevant administrative penalties.

10. 2 Sanctions

Administrative liabilities and sanctions are set forth as follows:

Administrative liability	Sanctions
Illegal operations with a natural person's data include: collection of data; registration entering; storing; ordering; transforming; utilisation; transfer; transmitting; blocking or deleting.	A warning or a fine imposed on natural persons in an amount from LVL 50 up to LVL 400; on officials from LVL 100 up to LVL 400; but for legal persons from LVL 1,000 up to LVL 8,000, with or without confiscation of the articles and tools used to commit the violation.
Illegal operations with a natural person's sensitive data include: collection of data; registration entering; storing; ordering; transforming; utilisation; transfer; transmitting; blocking or deleting.	A warning or a fine imposed on natural persons in an amount from LVL 200 up to LVL 500; on officials from LVL 300 up to LVL 500; but for legal persons from LVL 3,000 up to LVL 10,000, with or without confiscation of the articles and tools used to commit the violation.
Blocking a natural person's data; failure to follow an order regarding deletion or destruction of incorrectly or illegally obtained data; and continuing to process a natural person's data after a permanent or temporary prohibition on processing has been specified.	A fine imposed on natural persons in an amount from LVL 50 up to LVL 500; on officials from LVL 200 up to LVL 500, but for legal persons from LVL 1,000 up to LVL 10,000.
Failure to provide information specified by law to a data subject.	A warning or a fine imposed on natural persons in an amount from LVL 50 up to LVL 500; on officials from LVL 200 up to LVL 500; but for legal persons from LVL 1,000 up to LVL 5,000.
Processing a natural person's data without registration specified by law or without the registration of the personal data protection specialist at the DSI.	A warning or a fine imposed on natural persons in an amount from LVL 100 up to LVL 500; on officials from LVL 200 up to LVL 500; but for legal persons from LVL 1,000 up to LVL 10,000, with or without confiscation of the articles and tools used to commit the violation.

Failure to submit amendments regarding the personal data processing as specified by law to the DSI.	A warning or a fine imposed on natural persons in an amount from LVL 50 up to LVL 400; on officials from LVL 100 up to LVL 400; but for legal persons from LVL 800 up to LVL 8000.
Failure to provide the information provided for by the law, or the provision of false information to the DSI.	A warning or a fine imposed on natural persons in an amount from LVL 50 up to LVL 500; on officials from LVL 200 up to LVL 500; but for legal persons from LVL 1,000 up to LVL 5,000.
Failure to accredit the persons specified by law to the DSI.	A warning or a fine imposed on natural persons in an amount from LVL 50 up to LVL 500; on officials from LVL 200 up to LVL 500; but for legal persons from LVL 1,000 up to LVL 5,000.

The criminal liability regarding unlawful activities involving personal data of natural persons and sanctions is set forth as follows:

Criminal liability	**Sanction**
Unlawful activities involving personal data of a natural person, if it causes significant harm.	The deprivation of liberty for a term not exceeding two years, or custodial arrest, or community service, or a fine not exceeding 100 times the minimum monthly wage.
Unlawful activities involving personal data of a natural person, if they have been performed by a data controller or a data processor for the purpose of vengeance, acquisition of property or blackmail.	The deprivation of liberty for a term not exceeding four years, or custodial arrest, or community service, or a fine not exceeding 120 times the minimum monthly wage.
Influencing a data controller or a data processor or a data subject by using violence or threats or using trust in bad faith, or using fraud in order to perform unlawful activities with the personal data.	The deprivation of liberty for a term not exceeding five years, or custodial arrest, or community service, or a fine not exceeding 200 times the minimum monthly wage.

10.3 Examples of recent enforcement of data protection rules

Each year the DSI publishes its annual report, which can be used as a source of information on the DSI's activities as well as opinions and explanations regarding various matters related to personal data processing and protection. According to the latest report, in 2009 the DSI received 158 written complaints regarding potential violations in the field of personal data protection. In 2009, more complaints were submitted about the publication of personal data on the internet; video surveillance; data processing carried out by house managers when publishing information on delayed payments; debt collection; the transfer of factual and historical information regarding the collection of loans to third persons; activities of credit institutions when requesting, acquiring and transferring personal data; throwing out/abandonment in a publicly accessible place by any person of documents containing personal data either accidently or intentionally; and the use of personal data belonging to another person instead of one's own personal data.

In 2009, as the result of inspections carried out by the DSI regarding potential violations of the Law, administrative penalties were applied in 52 cases, of which there were 26 fines and 26 warnings. These cases related to the non-provision of information to the DSI (10 cases); the non-registration of personal data processing or its amendments to the DSI (four cases); non-provision of information to data subjects (two cases); and the rest related to illegal processing of personal data.

10.4 Judicial remedies

The Law explicitly provides that if due to violations of it, harm or loss are caused to a person, he or she is entitled to receive compensation accordingly. Likewise, a person may bring a claim and ask a court to either impose certain obligations on a person performing unlawful activities with personal data, or to prohibit or restrict certain activities with or in relation to such data. A person may also claim to compensate costs of adjudication, which are the court costs (for example, state fees) and costs related to conducting the matter (costs related to the legal assistance of attorneys at law). In addition, where applicable, a person may take advantage of such judicial remedies as securitisation of evidence or even securitisation of a claim.

10.5 Class actions

The laws of Latvia do not provide for the possibility of a class action, where it would be possible to start a legal procedure in order to, for example, protect specific data subjects or recognise particular data processing activities as illegal. Each person must bring a legal action to protect his or her particular legal interests, which have been jeopardised or violated in a particular situation.

10.6 Liability

With regard to civil liability, the Law explicitly provides that if, due to violations of the Law, harm or loss is caused to a person, he or she is entitled to receive compensation accordingly. In addition, where applicable, a particular person may be held liable accordingly and either administrative or even criminal sanctions can be imposed.

Luxembourg

Arendt & Medernach Héloïse Bock

1. LEGISLATION

1.1 Name/title of the law

The law of 2 August 2002 on the protection of persons with regard to the processing of personal data as amended (the Data Protection Law) implements Data Protection Directive 95/45/EC in Luxembourg.

Specific rules on the protection of persons with regard to the processing of personal data in the sector of electronic communications accessible to the public are contained in a separate law of 30 May 2005 as amended (the ePrivacy Law) which has been adopted as part of the implementation of the ePrivacy Directive.

1.2 Pending legislation

None.

1.3 Scope of the law

1.3.1 The main players

The main players under the Data Protection Law are defined as follows:
'Data subject': any natural person who is the subject of data processing of a personal nature.

'Controller': the natural person or legal entity, public authority, department or any other body which, alone or jointly with others, determines the purposes and means of the personal data processing; when the purposes and means of processing are determined by or pursuant to legal provisions, the controller is designated by the specific criteria in compliance with those legal provisions.

'Processor': a natural or legal entity, public authority, department or any other body that processes personal data on behalf of the controller.

'Third party': any natural person or legal entity, public authority, department or any other body, other than the data subject, the data controller, the data processor and the persons who, under the direct authority of the data controller or the data processor, are authorised to process personal data.

1.3.2 Types of data

Following the 2007 amendments of the Data Protection Law, the latter only applies to personal data concerning natural persons and excludes data concerning legal entities.

'Personal data' are defined as any information of any type regardless of the type of medium, including sound and image, related to an identified

or identifiable natural person; a natural person will be considered to be identifiable if he can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, genetic, mental, cultural, social or economic identity'.

In addition, the Data Protection Law distinguishes the following special categories of data:

- 'Sensitive data' are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health or sex life, including genetic data.
- 'Health data' are any information about the data subject's physical or mental state, including genetic information.
- 'Genetic data' are any data concerning the hereditary characteristics of an individual or group of related individuals.

1.3.3 Types of acts/operations

The Data Protection Law applies to the processing of personal data carried out either wholly or partly by automatic means and to the processing otherwise than by automatic means of personal data which form part or are intended to form part of a filing system as well as to any form of capture, processing and dissemination of sounds and images allowing the identification of natural persons.

The 'processing of personal data' is defined as any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

A 'personal data filing system' ('filing system') is defined as any structured set of data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

1.3.4 Exceptions

Data processing carried out by a person in the exclusive course of his personal or household activities falls outside the scope of the Data Protection Law.

1.3.5 Geographical scope of application

From a geographical point of view, the Data Protection Law applies:

- where the data processing is carried out by a data controller who is established on the Luxembourg territory; or
- where the processing is carried out by a data controller who is not established in Luxembourg or on the territory of any other member state of the European Union, but who makes use of processing resources located in Luxembourg, unless such resources are used only for purposes of transit through the said territory or the territory of another member state.

1.4 Particularities
None.

2. DATA PROTECTION AUTHORITY
Commission Nationale pour la Protection des Données / National Commission for Data Protection (CNPD)
41, avenue de la Gare ; L-1611 Luxembourg

2.1 Role and tasks
The duties of the CNPD are:
- to ensure the implementation of data protection rules;
- to control the lawfulness of data processing and inform data controllers of their obligations;
- to inform individuals of their fundamental freedoms and rights and ensure the respect of such rights;
- to advise the government regarding data protection issues;
- to examine requests from data subjects requesting the control of the lawfulness of data processing;

The CNPD is also in charge of the implementation of the ePrivacy Law provisions.

2.2 Powers
The CNPD has the following powers:
- a power of investigation in order to collect all the information necessary to fulfil its duties; for this purpose the CNPD benefits from a right of direct access to the premises other than residential premises where the data processing is undertaken as well as to the data processed;
- the right to be a party to legal proceedings, in particular the right to file a cessation action;
- the right to administer administrative sanctions.

2.3 Priorities
In 2010 the CNPD pursued its information and advisory duty towards private and public stakeholders through conferences, training programmes, occasional awareness campaigns or meetings on data protection issues. The CNPD also advised the lawmaker with regard to bills of law pertaining to data protection issues in the health or telecommunication sectors.

3. LEGAL BASIS FOR DATA PROCESSING
3.1 Consent
3.1.1 Definition
'Consent' is defined as 'any freely given, specific and informed indication of his wishes by which the data subject or his legal, judicial or statutory representative signifies his agreement to his personal data being processed'.

3.1.2 Form
The form of the consent is not specified by the Data Protection Law.

3.1.3 In an employment relationship

The Labour Code expressly provides that consent given by an employee does not constitute a valid legal basis for data processing for the purpose of surveillance at the workplace.

In view of the employee's subordination to the employer, the validity of the consent given by an employee may be put into question and it is advisable to rely on another legal ground for data processing.

3.2 Other legal grounds for data processing

Data processing may generally be carried out only if:

- it is necessary for compliance with a legal obligation to which the data controller is subject;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed;
- it is necessary for the performance of a contract to which the data subject is party or for the performance of pre-contractual measures taken at the request of the data subject;
- it is necessary for the achievement of the legitimate interests pursued by the data controller or by the third party to whom the data are disclosed, upon the condition that such interests are not overridden by the interests or the fundamental rights and freedoms of the data subject;
- it is necessary to safeguard the vital interests of the data subject; or
- the data subject has given his consent.

However, specific provisions apply to processing of specific categories of data. The processing of sensitive data is forbidden, unless one of the following exceptions apply:

- the data subject has given his explicit consent to such processing, except where this is prohibited by the law or where this falls within the inalienability of the human body;
- processing is necessary for the purposes of carrying out the obligations and specific rights of the data controller in the field of employment law in so far as it is authorised by law;
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
- processing is carried out with the consent of the data subject by a foundation, association or any non-profit-seeking body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the necessary data of members of that body or to persons who have regular contact with it in connection with its purpose and that the data are not disclosed to a third party without the consent of the data subjects;
- processing relates to data which are manifestly made public by the data subject;
- processing is necessary for the establishment, the exercise and the defence of a right;

- processing is necessary for a reason of public interest, notably for historical, statistical or scientific reasons;
- processing is implemented via a grand-ducal regulation; or
- processing is carried out in the context of the processing of judicial data.

Genetic data may only be processed:

- to verify the existence of a genetic link for the purpose of collecting evidence, for identification purposes, for the prevention or sanction of a specific criminal offence; or
- if the data subject has given his consent and if the processing is carried out only in the area of healthcare or scientific research subject to the inalienability of the human body and except where the law provides that the general prohibition cannot be lifted by the data subject's consent. In this case, the processing can only be carried out by medical authorities, or by research bodies or the natural or legal persons whose research project has been approved under the legislation applicable to biomedical research; or
- if the processing of genetic data is necessary for the purpose of preventive medicine, medical diagnosis or the provision of care or treatment. In this case, the processing of such data may only be carried out by the medical authorities.

Without prejudice to the application of the provisions concerning the processing of genetic data, data processing relating to health and sexual life is permitted in the following situations:

- if necessary for the purpose of preventive medicine, medical diagnosis or the provision of care or treatment by the medical authorities;
- if necessary for the purpose of healthcare or scientific research by the medical authorities, or by the research bodies or the natural or legal persons whose research project has been approved under the legislation applicable to biomedical research; or
- if necessary for the management of healthcare services by the medical authorities or, if the data controller is subject to professional secrecy, by social security bodies and authorities that manage the said data in performance of their legal and regulatory tasks, by insurance companies, pension fund management companies, the '*Caisse Médico-Chirurgicale Mutualiste*' and by those natural persons or legal entities authorised to do so by law for socio-medical or therapeutic reasons.

The processing of judicial data is permitted in the following situations:

- processing for the purpose of criminal investigations and legal proceedings shall be performed pursuant to the provisions of the Code of Criminal Procedure, the Code of Civil Procedure and the law relating to procedural regulations in administrative courts or other laws;
- processing of data relating to offences, criminal convictions or security measures may be carried out only in performance of a legal provision.

An exhaustive collection of criminal convictions can however only be held under the control of the competent public authority.

To the extent necessary to make the right to privacy compatible with the rules governing freedom of expression, data processing carried out solely for

journalistic, artistic or literary expression is not subject to:

- the prohibition of processing of specific categories of data as set out above and to the limitations concerning the processing of judicial data, if the processing is in connection with data that have manifestly been made public by the data subject, or concerns data which are directly related to his public life or to the event in which he is voluntarily involved;
- the condition of adequacy of the level of protection in the case of transfer of data to a third country (see section 8 below);
- the information obligation which applies when data are collected directly from the data subject if its implementation would compromise the collection of data;
- the information obligation which applies when data are not collected directly from the data subject if its implementation would compromise the collection of data or would compromise a future publication, the public disclosure of the data in any form whatsoever or would enable the identification of the sources of information;
- the data subject's right of access which is postponed and limited.

Regarding data processing for surveillance purposes, see section 3.6.1.

3.3 Direct marketing and cookies

Any data subject has the right to object, on request and free of charge, to the processing of his personal data for the purposes of direct marketing. It is the responsibility of the data controller to bring this right to the attention of the data subject.

The data subject must also be informed before his data are disclosed to or used for the first time by third parties for marketing purposes and be expressly offered, free of charge, the right to object to such disclosure or use.

With regard to cookies, the ePrivacy Law provides that the storing of information or the gaining of access to information already stored in the terminal equipment of a subscriber or a user may be allowed provided that the subscriber or the user has given his consent and that he was provided with clear and comprehensive information, inter alia about the purposes of the processing. When it is technically possible the subscriber or the user's consent can be expressed via the use of appropriate parameters of a browser or of another application.

3.4 Data quality requirements

The personal data processed must be:

- collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were collected and processed.

3.5 Outsourcing

When the data processing is delegated by the data controller to a data processor, such data processor must act under the authority of the data controller and upon his instructions. In addition, the data controller must ensure that the data processor provides sufficient guarantees in relation to the technical and organisational security measures pertaining to the processing to be carried out. It is the responsibility of both the data controller and the data processor to ensure that the said measures are respected.

The data controller and the data processor must enter into a written agreement that must provide in particular that:

- the data processor will act only on instructions from the data controller, and
- will be subject to the obligations concerning the security of processing operations.

3.6 Email, internet and video monitoring

3.6.1 General rules

Surveillance in general – including video recordings, monitoring of emails and the use of the internet – is defined by the Data Protection Law as any activity which, carried out using technical instruments, consists of observing, collecting or recording in a non-occasional manner the personal data of one or more persons, concerning behaviour, movements, communications or the use of electronic computerised instruments.

The processing of data for surveillance purposes may be carried out only:

- if the data subject has given his consent; or
- in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question, due to its nature, position, configuration or frequentation presents a risk that makes the processing necessary;
- for the safety of its users and for the prevention of accidents;
- for the protection of goods, if a clear risk of theft or vandalism exists;
- in private places where the resident natural or legal person is the data controller; or
- if the processing is necessary to safeguard the vital interests of the data subject or of another person if the data subject is physically or legally incapable of consenting to the processing.

Data processing for surveillance purpose requires prior authorisation from the CNPD (see section 6.2 below).

3.6.2 Employment relationship

Surveillance at the workplace is specifically regulated and may be carried out by the employer only if it is necessary:

- for the health and safety of employees;
- to protect the company's property;
- to control the production relating solely to machinery;
- to temporarily control production or the employee's services if such a

measure is the only way of determining the exact earnings;
- in connection with the organisation of work under a flexible hours scheme in accordance with the law.

Unlike the surveillance of non-employees, data controllers do not have the possibility of basing the surveillance of their employees on their consent.

Data processing for surveillance purposes at the workplace requires prior authorisation from the CNPD (see section 6.2 below) and is subject to an extended information obligation.

4. INFORMATION OBLIGATIONS

4.1 Who

The data controller is responsible for providing the information directly to data subjects.

4.2 What

When the data are collected directly from the data subject, the data controller must supply the data subject with the following information unless the data subject has already been informed of it:
- the identity of the data controller and of his representative, if any;
- the purpose(s) of the processing for which the data are intended;
- any further information such as:
  (i) recipients to whom the data might be disclosed;
  (ii) whether answering the questions is compulsory or voluntary, as well as the possible consequences of failure to answer; and
  (iii) the existence of the right of access to personal data and the right to rectify them, inasmuch as, in view of the specific circumstances in which the data are collected,

  this additional information is necessary to ensure the fair processing of the data in respect of the data subject.

Where the data have not been obtained directly from the data subject, the data controller must, in addition to the information listed above, provide the data subject with further information relating to the categories of data concerned, except where the data subject has already been informed of it and only if this additional information is necessary to ensure the fair processing of the data.

4.3 Exceptions

The obligation to provide information to data subject does not apply when the processing is necessary to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, including those relating to the fight against money laundering or to safeguard the course of other legal proceedings;
(e) an important economic or financial interest of the state or of the European Union,

including monetary, budgetary and taxation matters;

(f) the protection of the data subject or the protection of rights and freedoms of others;

(g) a monitoring, inspection or regulatory mission relating, even on an occasional basis, to the exercise of official authority in cases referred to in letters (c), (d) and (e);

It may be possible to derogate from the information obligation in cases of data processing for journalism or artistic or literary expression purposes when its implementation would compromise the collection of data from the data subject or would compromise a future publication, the availability of the said data to the public or would enable the identification of the sources of information.

The information obligation shall also not apply where, in particular for processing for statistical, historical or scientific purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure of data is expressly laid down by law.

4.4 When

When the data are collected directly from the data subject, the information must be provided no later than the time when the data are collected.

When the data have not been obtained from the data subject, the information must be provided at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

4.5 How

The Data Protection Law does not specify how the information must be provided. However, for reasons of evidence, the information should be provided in writing and the data controller should retain proof of the date and content of the information provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The right of access can be exercised by the data subject or by his beneficiaries having a legitimate interest to obtain such access. This right can be exercised by a request addressed to the data controller.

The right of access includes the right to obtain:

- access to personal data relating to the data subject;
- confirmation as to whether or not his data are being processed and information as to the purposes of the processing, the categories of data concerned and the categories of recipients to whom the data are disclosed;
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;
- knowledge of the logic involved in any automatic processing of his data.

Regarding the right of access of patients, it may be exercised by the

patient himself or by a doctor appointed by him. Following the patient's death, his spouse, his children and any other person who at the time of death was living with him as part of the household, or in the case of minors, his father and mother, may exercise the right of access via a doctor they have appointed.

The patient's right of access may be exercised during the lifetime of a person under guardianship or trusteeship via a doctor appointed by his guardian or trustee.

5.1.2 Exceptions

The controller may restrict or defer exercise of a data subject's right of access if such a measure is necessary in order to safeguard:

- national security;
- defence;
- public safety;
- the prevention, investigation, detection and prosecution of criminal offences, including those relating to the fight against money laundering, or to safeguard the course of other legal proceedings;
- an important economic or financial interest of the state or of the European Union;
- the protection of the data subject or the protection of rights and freedoms of others;
- a monitoring, inspection or regulatory mission relating, even occasionally, to the exercise of official authority in cases referred to in letters (c), (d) and (e);

The data controller may also limit the right of access in the event that there is obviously no risk of breaching the privacy of a data subject, when the data are being processed solely for the purposes of scientific research, or are stored in data form for a period which does not exceed the period necessary for the sole purpose of creating statistics and if the said data cannot be used for the purpose of taking a measure or a decision relating to specific persons.

In the context of the processing of personal data carried out for journalistic, artistic or literary expression, the data subject's right of access to his data is limited inasmuch as it may not cover information concerning the origin of the data which would allow the identification of a source.

In the case of limitation of the data subject's right of access, the right of access will be exercised by the CNPD on behalf of the data subject. In such case, the CNPD may request the rectification, erasure or blocking of data when the processing does not comply with the Data Protection Law.

5.1.3 Deadline

The Data Protection Law does not provide for a fixed deadline to exercise the right of access. Access to data must be granted in reasonable intervals and without excessive delay.

5.1.4 Charge

The right of access is free of charge.

5.2 Rectification

5.2.1 Right

The data subject has a right to request the rectification of data when the processing does not comply with the Data Protection Law, in particular because of the incomplete or inaccurate nature of the data.

5.2.1 Exceptions

There is no specific exception mentioned in the Data Protection Law. However if the right of access is limited, the right to request the rectification of data is also limited.

5.2.2 Deadline

The Data Protection Law does not provide for a particular deadline to exercise the right of rectification or to implement the rectification. However, once the data are corrected, the data controller must notify without delay the person who gained access to the data, unless it is impossible.

5.2.4 Charges

The right to request the rectification of data is free of charge.

5.3 Erasure

5.3.1 Right

The data subject has a right to request the erasure of data when the processing does not comply with the Data Protection Law, in particular because of the incomplete or inaccurate nature of the data.

5.3.2 Exceptions

There is no specific exception mentioned in the Data Protection Law. However if the right of access is limited, the right to request the erasure of data is also limited.

5.3.3 Deadline

The Data Protection Law does not provide for a particular deadline to request the erasure of data or to comply with the request. However, once the data have been erased, the data controller must notify without delay the person who gained access to the data, unless it is impossible.

5.3.4 Charges

The right to request the erasure of data is free of charge.

5.4 Blocking

5.4.1 Right

The data subject has a right to request the blocking of data when the processing does not comply with the Data Protection Law, in particular because of the incomplete or inaccurate nature of the data.

5.4.2 Exceptions

There is no specific exception mentioned in the Data Protection Law. However if the right of access is limited, the right to request the blocking of data is also limited.

5.4.3 Deadline

The Data Protection Law does not provide for a particular deadline to request the blocking of data or to comply with the request. However, once the data have been blocked, the data controller must notify without delay the person who gained access to the data, unless it is impossible.

5.4.4 Charges

The right to request the blocking of data is free of charge.

5.5 Objection

5.5.1 Right

Any data subject is entitled to object for compelling and legitimate reasons relating to his special situation to the processing of his data.

5.5.2 Exceptions

The right to object does not apply in cases where legal provisions expressly provide for that processing.

5.5.3 Deadline

This right can be exercised at any time.

5.5.4 Charges

The right to object to the processing of personal data for the purposes of direct marketing must be exercised free of charge (see section 3.3).

5.6 Automated individual decisions

5.6.1 Right

A decision which is based solely on automated processing of data and which produces legal effects concerning him is only permitted if such decision:

- is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view forward; or
- is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

5.6.2 Exceptions

Not applicable.

5.6.3 Deadline

The Data Protection Law does not provide for a particular deadline.

5.6.4 Charges
The Data Protection Law does not specify whether charges may apply.

5.7 Other rights
None.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
Data controllers are responsible for fulfilling the notification requirement.

6.1.2 What
The Data Protection Law provides for the obligation to notify the CNPD before undertaking any processing of personal data, unless the concerned data processing is exempted from the obligation of notification or falls under the authorisation obligation.

6.1.3 Exceptions
The Data Protection Law provides for various exceptions in which case a notification is not required. The most regularly used exceptions concern the data processing relating to:

- the administration of employees' wages, of employee recruitment and applications, or the management of employees working for the data controller;
- the data controller's accounting;
- the management of shareholders, bondholders and partners;
- the management of customers and suppliers;
- the management of data on visitors;
- the management of computer systems, networks and electronic communications.

The exemptions from notification are subject to certain conditions set out in the Data Protection Law (see also section 7.2 below).

6.1.4 When
Notification must be made before the corresponding data processing begins. The notification need not be renewed but any modifications must be notified. In addition, when the data processing is terminated, a form must be filed with the CNPD informing it of the end of the processing.

6.1.5 How
A notification must be made on the standard application form made available by the CNPD on its website.

The notification shall include at least the following information:

- the name and address of the data controller and of his representative, if any;
- the basis of legitimacy of the processing;
- the purpose(s) of the processing;

- a description of the categories of data subjects and of the data concerned;
- the recipients or categories of recipients to whom the data might be disclosed;
- the third countries to which it is proposed to transfer the data;
- a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure the security of processing.

Following completion of the form, the CNPD acknowledges receipt of the notification and publishes the notified processing in the public register. Since 2008, the CNPD has received approximately 300 to 400 notifications per year.

6.1.6 Notification fees

A fee of €125 is payable for a notification in paper form, and €100 for an electronic notification. Payment must be made to the CNPD before notification.

6.2 Authorisation requirements

6.2.1 Who

Data controllers are responsible for obtaining the required authorisation.

6.2.2 What

The following specific processing operations require prior authorisation from the CNPD:

- the processing of genetic data under certain circumstances;
- the processing of data for the purposes of surveillance in general if the data resulting from the surveillance are recorded and for the purpose of surveillance at the data subject's place of work;
- the subsequent processing of data for historical, statistical or scientific purposes;
- the combination of data;
- the processing of information relating to the credit status and solvency of data subjects if such processing is not carried out by professionals of the financial sector or insurance companies regarding their clients;
- the processing of biometric data necessary for identity controls; and
- the use of data for purposes other than those for which they were collected. Such processing may in any event be carried out only if prior consent is given by the data subject or if it is necessary to safeguard his vital interests.

Moreover, a transfer to a third country that does not provide an adequate level of protection may be authorised by the CNPD under certain conditions (see section 8 below).

6.2.3 Exceptions

The Data Protection Law does not provide for any exceptions to the authorisation requirements.

6.2.4 When

Authorisations must be obtained before the corresponding data processing begins and do not need to be renewed.

6.2.5 How

There is no standard form available for authorisation requests, except for requests regarding video monitoring or regarding transfer of data to third countries (these standard forms are available on the CNPD's website). With regard to requests for authorisation relating to data processing where no specific form exists, such request shall therefore be drafted in letter form.

The authorisation request shall include at least the following information:

- the name and address of the data controller and of his representative, if any;
- the basis of legitimacy of the processing;
- the purpose(s) of the processing;
- the origin of the data;
- a detailed description of the data or categories of data concerned and of the processing;
- a description of the categories of data subjects;
- the recipients or categories of recipients to whom the data might be disclosed;
- the third countries to which it is proposed to transfer the data;
- a detailed description allowing evaluation of compliance with the security measures.

Following the request for authorisation and provided all the conditions are fulfilled, the CNPD delivers the authorisation and publishes the authorised processing in the public register. Since 2008, the CNPD has received approximately 600 authorisation requests per year.

6.2.6 Authorisation fees

A fee of €125 is payable for a request for authorisation in paper form, and €100 for an electronic request. Payment must be made to the CNPD prior to the authorisation request.

6.3 Other registration requirements

None.

6.4 Register

The CNPD is responsible for keeping a public register of notified and authorised data processing. The register is accessible to everyone online.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The Data Protection Law offers the possibility for data controllers to appoint a data protection officer. However, such appointment is uncommon.

7.2 Tasks and powers

The powers of the data protection officer are the following:

- power of investigation to ensure supervision of the data controller's compliance with the legal provisions; and
- the right to be informed by the data controller and to inform the data controller of the formalities to be carried out in order to comply with the legal provisions.

By appointing a data protection officer, the data controller is exempted from the notification obligation of data processing which would otherwise apply. This exemption does not apply to processing for monitoring purposes.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Whereas data transfers to EU member states are not subject to specific restrictions provided that the other data protection provisions are fulfilled, data transfers to non-EU countries are only possible if the country in question is considered to ensure an adequate level of protection by the CNPD or the European Commission or if it falls under another legal exemption.

The adequacy of the level of protection afforded by a third country must be assessed by the data controller in the light of all the circumstances surrounding a data transfer operation, particularly the nature of the data; the purpose and duration of the processing; the country of origin and of final destination; the rules of law in force in the third country in question; and the professional rules and security measures which are complied with in that country.

8.2 Legal basis for international data transfers

The Data Protection Law expressly provides for the following legal bases for international data transfers.

- transfers to non EU-countries which offer an adequate level of protection.
- transfers to countries which are considered not to ensure an adequate level of protection may nevertheless take place provided that:
  (i) the data subject has given his consent;
  (ii) the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the data subject's request;
  (iii) the transfer is necessary for the conclusion or the performance of a contract concluded in the interest of the data subject between the data controller and a third party;
  (iv) the transfer is necessary to protect the vital interests of the data subject;
  (v) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
  (vi) the transfer is made from a register which, according to laws or

regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

The CNPD may authorise, as a result of a duly reasoned request, a transfer or set of transfers of data to a third country that does not provide an adequate level of protection 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.

8.2.1 Data transfer agreements

The European Commission's standard contractual clauses are commonly used in Luxembourg. The related data transfers still need to be authorised by the CNPD. In this regard, a permit application form (available online) must be filed with the CNPD together with the standard contractual clauses. The permit application form also provides for the possibility to use other contracts not approved by the European Commission such as the ones of the International Chamber of Commerce or the Council of Europe.

8.2.2 Binding corporate rules

Binding corporate rules are recognised in Luxembourg as ensuring an adequate level of protection, provided they have been duly approved by the CNPD. There is no specific form available online for such authorisation request. Luxembourg takes part in the European mutual recognition procedure. In 2010, two multinational companies requested the review of their binding corporate rules by the CNPD.

8.2.3 Safe Harbour

The US Safe Harbour certification is recognised in Luxembourg as ensuring an adequate level of protection. No prior authorisation of the CNPD is required.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Any person acting under the authority of the data controller or of the data processor, including the data processor himself, who has access to personal data must not process data except on instructions from the data controller, unless he is legally required to do so.

9.2 Security requirements

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

9.3 Data security breach notification obligation

The Data Protection Law does not provide for any general data security

breach notification obligation, although the CNPD recommends that data controllers notify data subjects of security breaches. In addition, the ePrivacy Law provides for a data security breach notification obligation which applies to the service providers of publicly available electronic communications services.

9.3.1 Who

The service providers of publicly available electronic communications services are responsible for complying with the notification obligation.

9.3.2 What

Notification is required in the event of a security breach.

9.3.3 To whom

The notification must be addressed to the CNPD and to the subscriber or individual concerned, in the event the security breach is likely to negatively affect his personal data or privacy. However, the CNPD may consider that the notification to individuals concerned is not necessary, provided the service provider has taken appropriate measures of technology protection which render the data incomprehensible to persons who are not authorised to gain access to such data.

9.3.4 When

The notification must be made without delay.

9.3.5 How

The notification to the subscriber or individual concerned shall include at least the nature of the data security breach, contacts where he can obtain more information and shall recommend actions which may reduce the possible negative consequences of the security breach.

The notification to the CNPD shall describe, in addition to the above information, the consequences of the security breach and the proposed measures or the measures already undertaken by the service provider to remedy such breach.

9.3.6 Sanctions for non-compliance

The first time the service provider does not comply with the notification obligation, it is only warned by the CNPD. In cases of repeated breaches, the CNDP may impose a fine which cannot exceed €50,000.

9.4 Data protection impact assessments and audits

There is no legal requirement to carry out data protection impact assessments and audits. However, the data controller must ensure that he complies with the Data Protection Law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Data Protection Law provides for the possibility to file a cessation action by virtue of which the competent judge may order the cessation of any processing that is contrary to the Data Protection Law and the temporary suspension of the activity of the data controller or data processor. Such an action may be filed by the state prosecutor, the CNPD or an injured party. The temporary closing down of the premises of the data controller or the data processor may also be ordered if the sole activity is the processing of data.

10.2 Sanctions

Breaches of nearly all aspects of the Data Protection Law are subject to criminal sanctions. The criminal sanctions for non-compliance with the Data Protection Law provisions consist of prison sentences, fines, and an order to discontinue the unlawful data processing.

The period of imprisonment may vary from eight days to six months or one year depending on the nature of the infringement. Fines range from €251 to €125,000.

In addition to the criminal sanctions that may apply, the CNPD may also impose the following administrative sanctions:

- alert or caution a controller who does not comply with the required subordination and security measures or who is in breach of its obligations relating to professional secrecy;
- block, delete or destroy data that have been subject to processing in breach of the legal provisions;
- impose a temporary or permanent ban on processing that is in breach of the legal provisions;
- order the publication of any decision that prohibits processing in whole or in part in newspapers or by any other method, at the expense of the offender.

10.3 Examples of recent enforcement of data protection rules

Please find below examples of enforcement of the Data Protection Law in 2010:

- The CNPD ordered the immediate suspension of a contest organised on a website, participation in which was conditional upon the communication of email addresses to be used for marketing purposes without the prior consent of the email account holders.
- Following the report to the CNPD of security flaws relating to different websites of internet or mobile telephone service providers allowing the foiling of authentication systems, the CNPD immediately sent a letter of formal notice to these service providers ordering them to disable the authentication features.

10.4 Judicial remedies

A data subject may enforce its rights under the Data Protection Law by filing a cessation action or by claiming damages, under certain circumstances, before civil courts or in the context of a criminal action when brought

simultaneously with a civil action, on the basis of the Civil Code provisions.

10.5 Class actions

Class actions do not exist as such under Luxembourg law.

10.6 Liability

The data controller also remains responsible for damages resulting from a breach of the Data Protection Law, even in the event he has appointed a data processor. Since March 2010, legal entities can also be held criminally liable.

Malta

GVTH Advocates Michael Zammit Maempel & Mark Hyzler

1. LEGISLATION

1.1 Name/title of the law

The principal law governing the collection and processing of personal data in Malta is the Data Protection Act, which makes up Chapter 440 of the Laws of Malta (the Act).

Subsidiary legislation has in turn been promulgated according to the terms set out in the Act itself in the form of Legal Notices. These are:

- Processing of Personal Data (Electronic Communications Sector) Regulations; Subsidiary Legislation 440.01.
- Notification and Fees (Data Protection Act) Regulations, Subsidiary Legislation 440.02.
- Third Country (Data Protection Act) Regulations, Subsidiary Legislation 440.03.
- Processing of Personal Data (Protection of Minors) Regulations, Subsidiary Legislation 440.04.
- Data Protection (Processing of Personal Data in the Police Sector) Regulations, Subsidiary Legislation 440.05.
- Processing of Personal Data (Police and Judicial Cooperation in Criminal Matters) Regulations, Subsidiary Legislation 440.06.

The implementation of the EU Directive 95/46/EC in Maltese legislation was carried out through the enactment of the Act, which was passed by the House of Representatives of Malta as Act XXVI of 2001 as subsequently amended by Act XXXI of 2002. The Act was brought into force on 15 July 2003.

1.2 Pending legislation

There is currently no draft legislation on the matter pending before the Maltese Parliament. The Office of the Information and Data Protection Commissioner, which is the Maltese data protection authority, has however signalled that regulations concerning the role of the Personal Data Representative, as envisaged in Article 31 of the Act, are to be published in the near future. It is likely that these regulations will be published in the form of a Legal Notice similar to those listed in section 1.1 above.

1.3 Scope of the law

1.3.1 The main players

The main players under Maltese data protection law are the following;

- The 'Minister' refers to the Minister of government who may from time to time be entrusted with the portfolio of freedom of information and

data protection. The Minister is granted the power, under the Act, to publish regulations to better carry out the provisions of the Act.

- The 'controller' or 'controller of personal data' is defined as a person, natural or legal, who alone or jointly with others determines the purposes and means of the processing of personal data.
- The 'processor' is defined as a person, natural or legal, who processes personal data on behalf of a controller.
- The 'personal data representative' is defined as a person, appointed by the controller of personal data, who shall independently ensure that personal data is processed in a correct and lawful manner.
- The 'data subject' is the natural person to whom the personal data relates.
- The 'recipient' means a person to whom personal data are provided; in this case, the Data Protection Act states that the Commissioner shall not be regarded as a 'recipient' if the data provided to him were for the purpose of performing supervision, control or audit which is a duty of the Commissioner to attend to.
- The 'third party' means a person, other than the data subject the controller of personal data, the personal data representative, the processor and such persons who under the direct responsibility of the controller of personal data or the processor are authorised to process personal data.

1.3.2 Types of data

Personal data

'Personal data' are defined as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Data relating to legal persons, such as companies, are therefore excluded from the scope of the Act.

Sensitive data

'Sensitive data' can be distinguished from 'personal data' in the sense that they relate to personal data which reveals information concerning the data subject's race or ethnic origin; political opinions; religious or philosophical beliefs; membership of a trade union or health, or sex life.

1.3.3 Types of acts/operations

The processing of personal data refers to any operation or set of operations which is taken in regard to personal data, whether or not it occurs by automatic means, and includes: the collection; recording; organisation; storage; adaptation; alteration; retrieval, gathering; use; disclosure by transmission; dissemination or otherwise making information available; alignment or combination; blocking; erasure; or destruction of such data.

The Act does not make any direct reference to the manual processing of

personal data but merely to automated processing. However, the provisions apply to 'such other processing where such personal data form part or is intended to form part of a filing system'. A 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

1.3.4 Exceptions

The Act does not apply in the following scenarios:

- Where the processing of personal data is carried out by the controller who is established in a third country, the Act shall not apply if the equipment is used only for purposes of transit of information between a third country and another such country.
- Any processing of personal data which is undertaken by a natural person in the course of a purely personal activity, falls outside the scope of data protection law in Malta.
- Any processing operations which concern public security; defence; state security (including the economic well-being of the country relating to security matters); and activities carried out by the state in areas of criminal law. In areas of criminal law, there are certain exceptions stated in Subsidiary Legislation 440.05 which relate to the processing of personal data in the police sector.

1.3.5 Geographical scope of application

Apart from being applicable to the whole geographical territory of the Maltese Islands, the Act applies also to the processing of personal data carried out in the context of the activities of an establishment of a controller in Malta or in a Maltese Embassy or High Commission abroad. It also applies to processing carried out when such controller is established in a third country, provided that the equipment used for the processing of the personal data is situated in Malta. A list of third countries is published under the Act from time to time, but broadly speaking refers to countries outside the EEA/EU that have not aligned themselves to the general provisions of Directive 95/46/EC.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Office of the Information and Data Protection Commissioner/Ufficcju tal-Kummissarju ghall-Informazzjoni u l-Protezzjoni tad-Data.
Airways House – Level 2, High Street, Sliema SLM 1549, Malta
T: (+356) 2328 7100
F: (+356) 2328 7198
E: idpc.info@gov.mt
W: *www.idpc.gov.mt*

2.1 Role and tasks

There is only one authority in Malta which is the Office of the Information and Data Protection Commissioner (the Commissioner). The principal task of the Commissioner is to protect the individual's right to privacy by ensuring the correct processing of personal data.

Under the Maltese Data Protection Act, the Commissioner has a central and distinctive role. He has a long tenure of office (five years) following which he may again be reappointed. Also, he has a distinct legal personality while being capable of entering into 'contracts, of acquiring, holding and disposing of any kind of property for the purposes of his functions, of suing and being sued, and of doing all such things and entering into all such transactions as are incidental or conducive to the exercise or performance of his functions under this Act'.

The Act empowers the Commissioner with several other functions. These vary from issuing directions and advice to the government on data protection matters, to instituting civil legal proceedings in cases where provisions of the Act have been or are about to be violated. The wording 'about to be violated' is an important notion since it gives the Commissioner an observer role as well as an executive or administrative one.

2.2 Powers

The powers and functions of the authority are vested in the personality of the Commissioner. These can be summed up as follows:

- to create and maintain a public register of all processing operations according to notifications submitted to him as specified in the Act;
- to exercise control and, either of his own motion or at the request of a data subject, verify whether the processing is carried out in accordance with the provisions of the Act or regulations made under it;
- to instruct the processor and controller to take such measures as may be necessary to ensure that the processing is in accordance with the Act or regulations made under it;
- to receive reports and claims from data subjects or associations representing them on violations of the Act or regulations made under it, to take such remedial action as he deems necessary or as may be prescribed under the Act, and to inform such data subjects or associations of the outcome;
- to issue such directions as may be required of him for the purposes of the Act;
- to institute civil legal proceedings in cases where the provisions of the Act have been or are about to be violated and to refer to the competent public authority any criminal offence encountered in the course of or by reason of his functions;
- to encourage the drawing up of suitable codes of conduct by the various sectors affected by the provisions of the Act and to ascertain that the provisions of such codes are in accordance with the provisions of the Act and for such purpose the Commissioner may seek the views of data subjects or their representatives;

- to take such measures as may be necessary so as to bring to the knowledge of the general public the provisions of the Act and for such purpose to give advice to any person where it is required;
- to order the blocking, erasure or destruction of personal data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller;
- to advise the government on any legislative measures that are required to be taken to enable him carry out his functions appropriately;
- to draw up annual reports of his activities at regular intervals, at least once a year, which reports shall be made public;
- at the request of a data subject to verify that the processing of the personal data in the interests of national or public security, defence, in the investigation of criminal offences, or in the interest of important economic or fiscal matters is compliant with the provisions of the Act or of any law as specified under the relevant article of the Act and in such a case the data subject shall be informed accordingly; and
- to collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties, in particular by exchanging all useful information, in accordance with any convention to which Malta is a party or other any international obligation of Malta.

Additionally, the Commissioner is vested with the powers and functions that emanate from the Freedom of Information Act (Chapter 496 of the Laws of Malta) – which has not yet been fully brought into force.

2.3 Priorities

The prime priority for 2011 was to amend the Processing of Personal Data (Electronic Communications Sector) (Amendment) Regulations through Legal Notice 239 of 2011.

Another priority in 2011 was to enable online penalty payments. This feature is now available online on the IDPC website.

For some time now the Commissioner has signalled that he plans to publish regulations regarding the role of personal data representative, and specifically the functions that this person is expected to fulfil, and the qualifications such person will need to attain in order to take on the role in question. To date these regulations have not been promulgated, which means that the role of the personal data representative remains somewhat unclear and defined almost entirely by the practitioners in the field.

Furthermore, at the time of writing, the Commissioner is also carrying out a consultation process with interested parties regarding the publication of guidelines concerning the credit-referencing sector.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Under the Act consent means 'any freely given specific and informed indication of the wishes of the data subject by which he signifies his agreement to personal data relating to him being processed'.

3.1.2 Form

Consent may be tacit or express. 'Tacit consent' refers to consent that is implied through circumstances, or otherwise not in written form. 'Express consent' is typically interpreted to mean that consent has been granted in writing and under the data subject's signature or that of his legal representative.

Generally speaking, the data subject's consent must be sought and obtained prior to the commencement of the processing, except in the case of direct marketing, as will be explained in section 3.3 below.

3.1.3 In an employment relationship

Although consent must be freely given, it has become customary for written employment contracts to contain a blanket clause that governs the processing of all necessary employee data by the employer, for the purposes of that employment, and at least for the duration of the employment. Employers are required by Maltese law to retain fiscal-related data concerning employees even after the termination or expiry of their employment, and in some instances for up to eight years after such termination/expiry. Employers are exempted from seeking employee consent in such areas.

3.2 Other legal grounds for data processing

Sensitive personal data may be processed if appropriate safeguards are adopted and the processing is necessary to enable the controller to comply with his duties or exercise his rights under any law regulating the conditions of employment.

3.3 Direct marketing and cookies

The general rule laid down in the Act is that the data subject's consent must be sought and obtained prior to the commencement of the processing activity. In the case of direct marketing, controllers are not permitted to process personal data if the data subject gives notice to the controller that he opposes such processing. The controller has the duty to inform the data subject of his right to oppose, at no cost, processing for direct marketing purposes.

Consent, therefore, is based on an 'opt-out' model, as opposed to the general rule, which is based on an 'opt-in' premise.

With regard to the use of cookies, Malta has implemented Directive 2009/136/EC, which regulates the use of cookies in electronic communications, by means of Legal Notice 239/2011, which was published in the Malta Government Gazette on 24 June 2011.

3.4 Data quality requirements

Under the Maltese Data Protection Act the controller shall ensure that:

- personal data are processed fairly and lawfully;
- personal data are always processed in accordance with good practice;

- personal data are only collected for specific, explicitly stated and legitimate purposes;
- personal data are not processed for any purpose that is incompatible with that for which the information is collected;
- personal data that are processed are adequate and relevant in relation to the purposes of the processing;
- no more personal data are processed than is necessary having regard to the purposes of the processing;
- personal data that are processed are correct and, if necessary, up to date;
- all reasonable measures are taken to complete, correct, block or erase data to the extent that such data are incomplete or incorrect, having regard to the purposes for which they are processed;
- personal data are not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

3.5 Outsourcing

The processing of data may be outsourced by the data controller to third parties, who are subsequently defined as 'data processors'. The data processor is, broadly speaking, expected to process the data with the same degree of diligence and care as though he were the data controller himself. The law also obliges the controller to enter into a written agreement with the data processor regarding this outsourcing function, clearly with the aim of ensuring that the requirements and standards set out by the law are maintained and enforced effectively. Such written agreement must bind the processor to only act on instructions from the controller, and must ensure that the processor can implement the security measures that are to be adopted, and actually provide for this to take place.

Although processing agreements are typically drawn up on an *ad hoc* basis depending on the nature of the commercial relationship between the controller and processor, a sample agreement is available for download from the Commissioner's website (*www.idpc.gov.mt*).

3.6 Email, internet and video monitoring

3.6.1 General rules

The general principles laid out in the Act apply equally in the field of electronic communications such as email and other forms of internet communications. Additionally, the Processing of Personal Data (Electronic Communications Sector) Regulations (Legal Notice 16/2003 as amended) restrict the interception of such electronic communications, including data that are in transit, or traffic data.

The same general principles apply to CCTV imaging and video monitoring. The Commissioner has however released guidelines concerning the installation and use of CCTV equipment which stipulate that the general public is to be adequately warned of the presence of such CCTV equipment in any public or private place to which the public has or may have access.

3.6.2 Employment relationship

Maltese law is silent on this particular area of law, and consequently the general principles laid down by the Act also apply in this area.

4. INFORMATION OBLIGATIONS

4.1 Who

The controller or any other person authorised by him on his behalf must provide a data subject with information concerning the processing of their personal data.

4.2 What

The controller, on request and unless the data subject is already aware of this, must provide the data subject with the following information:

- the identity and habitual residence or principal place of business of the controller and of any other person authorised by him in that role, if any;
- the purposes of the processing for which the data are intended; and
- any further information relating to matters such as:
  (i) the recipients or categories of the recipients of data;
  (ii) whether the reply to any questions made to the data subject is obligatory or voluntary, as well as the possible consequence of failure to reply; and
  (iii) the existence of the right to access, the right to rectify, and, where applicable, the right to erase the personal data concerning him, and, insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

4.3 When

Information should be provided at the point at which the data subject's consent for processing is sought, or at any point further to that when the parameters for processing are substantially altered.

4.4 How

Maltese law merely states that requests for information from the data subject shall be provided in 'an intelligible form'.

5. RIGHTS OF INDIVIDUALS

5.1 Access

Data subjects have the right to request access to their personal data.

5.1.1 Right

Article 21 of the Act states that the controller of personal data at the request of the data subject shall provide to the data subject, without excessive delay and without expense, written information as to whether personal data concerning the data subject are processed:

If such data are processed the data controller shall provide to the data subject written information in an intelligible form about:

(i) actual information about the data subject which is processed;

(ii) where this information has been collected;
(iii) the purpose of the processing;
(iv) to which recipients or categories of recipients the information is disclosed; and
(v) knowledge of the logic involved in any automatic processing of data concerning the data subject.

5.1.2 Exceptions

The right of access shall not apply when a law specifically provides for the provision of information as a necessary measure in the interests of:

- national security;
- defence;
- public security;
- the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- an important economic or financial interest including monetary, budgetary and taxation matters;
- a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority
- such information being prejudicial to the protection of the data subject or of the rights and freedoms of others.

Furthermore the right of access shall not apply when personal data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics.

5.1.3 Deadline

The Act states that requests by data subjects for information shall only be made by the data subject 'at reasonable intervals' but does not define this phrase further – thereby leaving the matter largely to the discretion of the controller.

5.1.4 Charges

Requests for information are to be met without charge for the data subject.

5.2 Rectification

5.2.1 Right

The right to rectification of incorrect data is available to all data subjects in relation to data controllers processing such data.

5.2.2 Exceptions

No exceptions are contemplated by Maltese law in this regard.

5.2.3 Deadline

Maltese law is silent on this point and does not set out any deadline during which a request is to be made or entertained. It is fair to assume, however, that any such request should be acceded to without unreasonable delay.

5.2.4 Charges

Maltese law states that the controller is liable to rectify, block or erase personal data at the request of the data subject. This therefore implies that the data controller is also liable to foot the bill for any costs that may be necessary to do so, and that no charge is to be levied on the data subject.

5.3 Erasure

The same rules for rectification of data apply *mutatis mutandis* to the erasure of data.

5.4 Blocking

The same rules for the rectification of data apply *mutatis mutandis* to the blocking of data.

5.5 Objection

5.5.1 Right

Any data subject enjoys the right at all times to object to the processing of personal data by revoking his consent – originally given at the time the processing commenced. Generally speaking, consent is to be revoked in the same manner in which it was granted, which is to say that written consent is to be revoked in written form, whereas tacit consent may also be revoked tacitly. For the avoidance of doubt, it is customary for consent to be revoked in written form.

This right to object goes over and above the general rule established in direct marketing practices, where the data subject is at all times offered the right to opt out of further processing.

5.5.2 Exceptions

The data subject does not enjoy the right to object to the processing of personal data, where this is necessary for the performance of a legal or contractual obligation by the controller to which the data subject is a party.

Similarly, personal data may be processed regardless of the data subject's consent (or lack thereof), as a necessary measure in the interests of:

- national security;
- defence;
- public security;
- the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- an important economic or financial interest including monetary, budgetary and taxation matters;
- a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority; or
- such information being prejudicial to the protection of the data subject or of the rights and freedoms of others.

5.5.3 Deadline

There is no mention of any deadline in Maltese law in connection with this point.

5.5.4 Charges

Maltese law is entirely silent on this point.

5.6 Automated individual decisions

5.6.1 Right

The right to information about the logic regarding automated processing is available to all data subjects who are subject to a decision based on such automated processing, which decision produces legal effects or otherwise materially affects the data subject.

The data subject also enjoys the right to request that the decision be reconsidered other than in a manner based solely on automated processing, and such reconsideration shall be obligatory on the person making such decision.

5.6.2 Exceptions

The right to information does not apply where the decision is taken in the course of the entering into or performance of a contract with the data subject, provided that the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests such as the right to be heard.

5.6.3 Deadline

No deadline is laid down under Maltese law.

5.6.4 Charges

The data subject may not be charged for exercising his rights in this respect.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The controller shall notify the Commissioner before carrying out any wholly or partially automated processing operation or set of such operations intended to serve a single purpose or several related purposes.

6.1.2 What

The notification must specify:

- the name and address of the data controller and of any other person authorised by him in that role, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the personal data might be disclosed;

- proposed data transfers of data to third countries; and
- a general description allowing a preliminary assessment to be made of the appropriateness of the measures to ensure security of processing,

provided that the controller shall notify the Commissioner of any changes affecting the information and the Minister may prescribe any matter related to the form of such notification.

The controller shall notify the Commissioner about the appointment or removal of a personal data representative.

6.1.3 Exceptions

Where a personal data representative has been appointed according to the provisions of the Act, the controller shall submit the notification and the relevant fee with such personal data representative, who shall in turn, not later than seven days from the receipt of such notification, forward the notification documents and the relative payment to the Commissioner.

Furthermore, where the only personal data processed by a company are limited to the personal data contained in its memorandum and articles of association, which are registered with the Maltese Registrar of Companies, then such company is exempt from the obligation to notify.

Lastly, although not exempt from the obligation to notify, the Notification and Fees (Data Protection Act) Regulations (Legal Notice 154/2003 as amended) stipulate that the following persons are exempt from the notification fee and subsequent annual renewal fees laid down in the Act:

- any person who carries on a trade, business, profession or other economic activity in a self-employed capacity, but does not employ any people;
- any of the following organisations which are exempt from tax under the Income Tax Act (Chapter 123 of the Laws of Malta):
  (i) philanthropic institutions and other similar organisations;
  (ii) *bona fide* band clubs;
  (iii) *bona fide* sports clubs and other similar institutions;
  (iv) registered trade unions; and
  (v) political parties and clubs adhering to political parties.

6.1.4 When

Notification shall take place prior to the commencement of processing operations by the controller.

6.1.5 How

The Act does not specify the language in which notification is to take place, but the Constitution of Malta stipulates that both Maltese and English are to be considered equal and official languages, although Maltese alone is the national language.

Notification typically takes place in English and may either occur in hard copy by means of a form that is available online from the website of the Commissioner, or may otherwise take place by submitting an electronic form via the same website, which also processes online payments. The form

itself is a fairly comprehensive document that collects all the information required of the controller under the Act.

Notification forms are typically handled in a trouble-free fashion, and response from the Commissioner is typically swift and efficient, with acknowledgement and receipt usually received within 24 hours of submission. Notification forms are reviewed by the Commissioner and where elaboration or clarification is necessary, this is pointed out from their end. Once approved, a synthesis of the notification form is uploaded onto the online register of data controllers on the Commissioner's website, enabling the public to search data controllers by name, and also to view what fields of data and what data processes are being handled by that controller.

Amendments/additions to the original notification forms may also be effected online or in hard copy.

The Commissioner's website, including the public register of data controllers, may be viewed at *www.idpc.gov.mt*.

6.1.6 Notification fees

Notification fees are set at €23.29 per notification. A renewal fee of the same amount falls due each year on 15 July.

No fees are due for any amendment/additional forms that are entered at any later date.

Furthermore, there is no distinction between online submissions and hard copy submissions insofar as notification fees are concerned.

6.2 Authorisation requirements

6.2.1 Who

No licence or specific authorisation is required by data controllers in order to operate, apart from the notification obligations outlined above. However, controllers may require specific authorisation from the Commissioner in the case of transmission or transfer of data to a non-EEA country that does not provide an adequate level of protection or compliance with Directive 95/46/EC.

6.2.2 How

Requests for authorisation are handled on a case-by-case basis, and the Commissioner typically require that the exact nature of the request be submitted by means of a form prepared from their end, which is not available on the Commissioner's website. Requests are dealt with the Commissioner's customary efficiency, but with due care and scrutiny exercised at all times. So long as all the relevant information is submitted by the data controller together with the original request, the process to obtain this authorisation may sometimes be completed within the matter of a few days.

6.2.3 Authorisation fees

There are no fees for obtaining such authorisations.

6.3 Register

The Commissioner maintains a register of processing operations. The register contains the notification information submitted by the various data controllers. It is available for public consultation via the Commissioner's website *www.idpc.gov.mt*.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

There is no obligation under Maltese law to specifically appoint a data protection officer, although in those cases where the data controller is a legal person, the contact details of a natural person are to be submitted on the notification form.

Malta has recognised the concept of the appointment of a Personal Data Representative – meaning a person, appointed by the controller of personal data, who independently ensures that the personal data are processed in a correct and lawful manner.

7.2 Tasks and powers

The personal data representative shall have the function of independently ensuring that the controller processes personal data in a lawful and correct manner and in accordance with good practice and in the event of the personal data representative identifying any inadequacies, he shall bring these to the attention of the controller.

If the personal data representative has reason to suspect that the controller has contravened the provisions applicable for processing personal data and if rectification is not implemented as soon as practicable after such contravention has been pointed out, the personal data representative shall notify this situation to the Commissioner.

The personal data representative shall also consult with the Commissioner in the event of doubt about how the rules applicable to processing of personal data are to be applied.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The transfer to a third country of personal data that are undergoing processing or intended processing, may only take place subject to the provisions of the Act and provided that the third country to which the data are transferred ensures an adequate level of protection.

The adequacy of the level of protection of a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

It is for the Commissioner to decide whether a third country ensures an adequate level of protection.

The transfer of personal data to a third country that does not ensure adequate protection is prohibited.

8.2 Legal basis for international data transfers

The Act states that personal data may only be transferred to an unsafe third country if the data subject has given his unambiguous consent to the proposed transfer or if the transfer:

- is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the controller and a third party;
- is necessary or legally required on public interest grounds, or for the establishment, exercise or defence of legal claims;
- is necessary in order to protect the vital interests of the data subject; or
- is made from a register that according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, provided that the conditions laid down in law for consultation are fulfilled in the particular case.

8.2.1 Data transfer agreements

There is no prescribed form for data transfer agreements which are typically drafted on an *ad hoc* basis according to the nature of the dealing in question.

8.2.2 Binding corporate rules

Maltese law is silent on this point.

8.2.3 Safe Harbour

Data transfers to entities that have been certified under the US Safe Harbour scheme do not require authorisation, and these transfers are treated on a par with transfers within EEA territory. Notice of such transfer must nevertheless be made to the Commissioner in the form of a notification – either at startup, or at the point when the data process requiring such transfer arises.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data may only process personal data in accordance with instructions from the controller unless the person is otherwise required to do so by Maltese law. This includes the duty to treat all data with the topmost confidentiality and security.

9.2 Security requirements

The Act stipulates that the controller shall implement appropriate technical

and organisational measures to protect the personal data that are processed against accidental destruction or loss or unlawful forms of processing thereby providing an adequate level of security that gives regard to:

- the technical possibilities available;
- the cost of implementing the security measures;
- the special risks that exist in the processing of personal data; and
- the sensitivity of the personal data being processed.

If the controller engages a processor, the controller shall ensure that the processor:

- can implement the security measures that must be taken; and
- actually takes the measures so identified by the controller.

9.3 Data security breach notification obligation

Maltese law is silent on the question of whether a data controller has a duty to notify the Commissioner or indeed data subjects if there has been a security breach and personal data may have been compromised. While the Commissioner has always advocated the implementation of 'best practice' standards in the processing and storage of personal data, to date this is not reflected in the law.

9.4 Data protection impact assessments and audits

Maltese law places no obligation on the controller to carry out data protection impact assessments or audits; but the local reality has been influenced by the willingness of most entities to appoint a personal data representative as a form of 'audit figure' for this purpose. Market practice has shown that most commercial organisations are happy to appoint a personal data representative (usually provided by their external lawyers, or their external financial auditors) who provides a one-stop-shop service for their data protection requirements. Data audits are a common practice among medium to large companies, but understandably less common in smaller setups which handle far fewer data processes.

As signalled earlier, regulations or guidelines outlining the role of the personal data representative are eagerly awaited from the Commissioner, and when eventually published, are likely to include data protection audits as a role to be assumed by the personal data representative.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Commissioner is empowered by law to 'issue such directions as may be required of him for the purposes of this Act', which means that the Commissioner is authorised by law to take any action or issue any orders that may be necessary to ensure compliance with the provisions of the Act, provided, of course that any such directions or orders are based on the principles of natural justice. Additionally, the Commissioner is also empowered to institute civil proceedings 'where the provisions of this Act have been or are about to be violated' and in those cases where a criminal offence is encountered in the course of or by reason of his functions, then

the Commissioner may also refer the matter to the competent public authority (such as the Police) for action to be taken accordingly.

The Act empowers the Commissioner to obtain right of access to information that is requested; to seek rectification of personal data that is being processed incorrectly or unlawfully, and to block further data processing from taking place if the necessity so dictates; and to order a data controller to erase personal data that has been processed unlawfully.

Judicial proceedings initiated by the Commissioner, either before the civil or the criminal courts, have proved to be an extremely rare occurrence in Malta. Breaches of the law are typically handled by the Commissioner and its decisions are typically adhered to by those concerned, although on occasion an appeal against these decisions has been entered by one or more of the parties in question.

10.2 Sanctions

The Act provides for a series of administrative offences that are subject to penalties consisting of a fine not exceeding €23,293.73 or to imprisonment for six months, or to both such fine and imprisonment. These offences consist of:

- the providing of untrue information to data subjects as prescribed by the Act, or in the notification to the Commissioner, or to the Commissioner when the Commissioner requests information;
- the processing of personal data contrary to the provisions of the Act;
- the transfer of personal data to a third country contrary to the provisions of the Act (ie, unsafe third countries);
- the failure to notify under the Act or of any Regulations promulgated by its authority.

The Maltese Criminal Code (Chapter 9 of the Laws of Malta) furthermore lists a number of criminal offences concerning the misuse of computer equipment. Offences falling within this group of offences include, *inter alia*, the accessing of personal data without due authorisation, and the breaching of security systems in order to access such data either by hacking into a computer network, or by using login data that the offender is not authorised to use. These offences are penal in nature, meaning that the perpetrator must be brought before the criminal courts of Malta and prosecuted accordingly. The Commissioner therefore enjoys no jurisdiction over such offences, and may only refer the matter to the police or any other competent authority should these offences result during the course of an investigation.

Another particularity of the Act is the possibility of criminal offences apart from merely administrative ones, and from which terms of imprisonment may effectively be meted out by the Criminal Courts of Malta. The Act lists the offences that may attract a fine not exceeding €23,300 or a term of imprisonment not exceeding six months, or both.

10.3 Examples of recent enforcement of data protection rules

Ever since its inception, the Commissioner has adopted a policy of gentle but determined persuasion in implementing and enforcing data privacy laws

in Malta, rather than a policy of heavy-handed inspections and streams of judicial proceedings. This has made for a smoother, albeit slower, execution of the law and its obligations amongst the Maltese public and particularly within the Maltese business community.

The downside to this approach is principally that there are hardly any court judgments or decisions that have shaped the law and its interpretation in any significant manner, and consequently there is very little local authoritative material by which to go. Certainly, however, the law is being enforced and applied as Maltese citizens grow increasingly aware of their rights at law, and file a healthy number of complaints with the Commissioner. Although no official statistics exist concerning the exact number of complaints and investigations carried out by the Commissioner per month, it is the authors' experience as practitioners in the field to deal with a steady number of cases where commercial clients are asked to provide a statement of defence and proof of compliance to the Commissioner's office further to complaints registered by aggrieved individuals with that same office. In the past year, the authors have represented clients including Malta's ruling political party, hotel and catering establishments, credit referencing agencies, workers' co-operatives, medical patients, and A-list Hollywood celebrities who were engaged in film productions in Malta.

Perhaps the only two significant court judgments in recent years in Malta concerning the question of data privacy in telecommunications were those in the names of *Vodafone Malta Limited v Kummissarju ghall-Protezzjoni tad-Data* (Civil Appeal No. 16/2006), decided by the Civil Court of Appeal on 3 October 2007, and the concurrent case in the names *Mobisle Communications Limited v Kummissarju ghall-Protezzjoni tad-Data* (Civil Appeal No. 15/2006) decided on the same day by the same Court of Appeal.

These two cases were instituted by the two mobile network operators in Malta at the time: Vodafone Malta Limited and Mobisle Communications Limited against the Commissioner for Data Protection. The cases were virtually identical in substance and centred on data requested by the police from either mobile network company in the course of criminal investigations on a spate of arson attacks that took place in Malta, including attacks on two public figures. The Commissioner had sanctioned the release of this data by the mobile networks in question in favour of the Police, but the mobile networks had appealed against this decision claiming that the data requested would jeopardise their respective subscribers' privacy rights due to the fact that the data requested were imprecise, non-specific and needed to be extrapolated in order to be used – it left the data subjects completely unprotected in the context of the enormous powers held by the police over that data once under their control. The Commissioner had justified his decision on the basis that the data in question could only be used for the purposes of the police investigation in question and for no other purpose, and the Data Protection Appeals Tribunal had confirmed this decision. The Court of Appeal, however, overturned these earlier decisions and ruled that there was no justification for the police to be handed an inordinately huge volume of data, including those of persons

who were not even remotely connected with the investigation in question, particularly in view of the fact that this data request was not the only course of investigation that was being pursued, and that there were several other alternative avenues for investigation available to the police. Consequently, the subscribers' right to privacy, as laid out in Article 8(2) of the European Convention on Human Rights deserved to be upheld, given that there was no justifiable reason for limiting that right to privacy in the given circumstances.

10.4 Judicial remedies

As outlined in section 10.1 above, the Commissioner enjoys the right to initiate judicial proceedings before the civil courts, which are also competent to hear and decide on administrative law matters, against any entity or individual 'where the provisions of this Act have been or are about to be violated'.

Should any criminal offence be uncovered during the course of any investigation carried out by the Commissioner, it should be noted that the Commissioner may not initiate proceedings before a criminal court himself, but may only refer the matter to the competent investigating authority, such as the police, who may then in turn initiate proceedings themselves.

10.5 Class actions

Other than the two cases reported in section 10.3 above, and which were effectively constituted as class actions by all Malta's mobile network operators at the time, there are no other known cases of the sort. There is, however, nothing in Maltese law that impedes the filing of class actions so long as each plaintiff to a suit proves to have a juridical and personal interest in the suit in question.

10.6 Liability

The data subject may exercise an action for damages against the controller who processes data in contravention of the Act or regulations made under it. Such action is barred by the lapse of 12 months from the date when the data subject becomes aware, or could have become aware of such a contravention – whichever is earlier.

There appear to be no recorded cases of any aggrieved data subjects who have ever filed an action before the civil courts on the basis of the relevant Article of the Act. This is not surprising, particularly in light of the fact that the Maltese law on damages and compensation adopts a very strict approach where moral damages are not considered to be admissible, and consequently a plaintiff must prove real and actual losses in financial terms in order to successfully be awarded compensation.

Mexico

Dumont Bergman Bider & Co S.C.
Laura Collada & Jorge Molet

1. LEGISLATION

1.1 Name/title of the law

The Federal Law on the Protection of Personal Data held by individuals (LPPD), published in the Official Journal of the Federation (*Diario Oficial de la Federación*) (DOF) on 5 July 2010, entered into force on the day following its publication. This law is the result of the amendment to Article 73 section XXIX-O, published in the DOF on 30 April 2009, and Article 16, published on 1 June 2009, both from the Political Constitution of the United Mexican States.

The LPPD provides the regulatory framework for the whole country in the field of the protection of personal data and, in accordance with the Third Transitory Article abrogates all local regulations on the protection of personal data in the possession of individuals which were previously issued in Mexico. The LPPD comprises 69 Articles, divided into 11 chapters.

In addition to the Constitution and the LPPD, specific laws also contain provisions on the protection of privacy and personal data, such as:

- the Federal Law on Copyright, published in the DOF on 24 December 1996;
- the Federal Law on Consumer Protection, published in the DOF on 24 December 1992;
- the Law for Regulating Credit Information Societies, published in the DOF on 15 January 2002; and
- the Federal Law of Transparency and Access to Public Government Information, published in the DOF on 11 June 2002.

1.2 Pending legislation

The Third Transitory Article in the LPPD establishes that the Federal Executive Authority (the Authority) shall issue the regulations under the law (Regulations) within the year following its entry into force. The deadline for issuing the Regulations was 6 July 2011. At the time of the publication of this book, the Regulations were in the process of public consultation before the Federal Commission for Regulation Improvement (*Comisión Federal de Mejora Regulatoria*) (COFEMER), which is the government body commissioned with reviewing the various regulations proposed by government agencies and ensuring that the benefits of applying a new regulation outweigh the costs caused by its implementation.

The preliminary draft of the Regulations under the LPPD proposes to define with greater breadth different aspects of the law for developing,

complementing and detailing its content related to the principles, rights and obligations established by the LLPD, with special attention to sensitive data, self-regulation and the procedures toward the protection of rights, verification and imposition of sanctions.

1.3 Scope of the law

1.3.1 The main players

- The 'data subject' (also known as the 'data holder') is 'any natural person to whom personal data correspond'.
- The 'data controller' (also known as 'individual responsible') is 'any natural or legal person in private who has the capacity to make decisions on the treatment of personal data'.
- The 'data processor' is 'any natural or legal person who alone or jointly with others processes personal data on behalf of a data controller'.
- The 'third party' is 'any natural or legal person, domestic or foreign, other than the data holder or the data controller'.
- The 'personal data department' is the human person or department which must process data subjects' applications to put their rights into practice. Furthermore, it has the obligation to encourage the protection of personal data within the organisation.

1.3.2 Types of data

'Personal data' are defined as 'any information relating to an identified or identifiable natural person' and include an individual's name, address, telephone number, email, address, etc.

The LPPD distinguishes two categories of special personal data that are subject to stricter processing conditions:

(i) Sensitive data are 'the personal data that affect the most intimate sphere of its subject, or whose misuse could cause discrimination or carry a serious risk. In particular, sensitive data are those which may reveal aspects such as racial or ethnic origin, current and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views and sexual orientation.'

(ii) Financial or property data, which are not defined by the LPPD yet.

The LPPD only covers personal data relating to natural persons and not legal persons (companies).

The LPPD defines the term 'dissociation' as the 'procedure by which personal data may not be associated with the data subject or to allow, by its structure, content, or degree of disaggregation, the identification of the same'. The personal data which are submitted to a process of dissociation do not require the consent of the data subject for their treatment.

1.3.3 Types of acts/operations

The LPPD defines the term 'treatment' or 'processing' of data as any collection, use, disclosure or storage of personal data by any means, whether manual, automated, digital or by any other technology now known or to be known. The LPPD also provides examples of the use of personal data as

any action to access, manage, use, transfer or dispose of personal data. This means that treatment or processing includes any operation or handling of personal data, from procurement through cancellation and suppression.

The LPPD also defines the term 'database' as the ordered set of personal data referring to an identified or identifiable natural person, which do not require any authorisation for their creation. However, in the case of sensitive databases, these may not be created without a justification for their existence based on legitimate and concrete grounds in accordance with the activities or individual goals pursued by the creator of the database.

1.3.4 Exceptions

Specific exceptions for compliance with the LPPD are as follows:

(i) databases created by people who collect and store personal data for personal use only, without any non-disclosure or use for commercial purposes;

(ii) credit information companies, as long as there is a specific law governing the protection of data processed by these companies.

1.3.5 Geographical scope of application

The LPPD is mandatory throughout the entire Mexican Republic. The law does not provide or set any other applications involving the processing of personal data. However, the draft regulations currently under public consultation propose its mandatory application in different scenarios.

1.4 Particularities

An interesting feature about the LPPD in Mexico is that the approval from the Mexican data protection authority (IFAI) in the field of protection of personal data is not required for the creation of non-sensitive databases or for carrying out transfers of databases. However, such operations must nonetheless comply with the requirements set forth by the LPPD, providing evidence of such compliance.

2. DATA PROTECTION AUTHORITY

The Federal Institute for Access to Public Information and Data Protection (*Instituto Federal de Acceso a la Información Pública y Protección de Datos* (IFAI)).
Av. México No. 151, Colonia El Carmen, Coyoacán, C.P. 04100, Delegación Coyoacán, México D.F.
T: (+52 55) 5004 2400. Ext. 2595 / 2596.
E: atencion@ifai.org.mx
W: *www.ifai.org.mx*

2.1 Role and tasks

The IFAI, which is the data protection ministry, is the agency of federal public administration with operational, budgetary and decision-making autonomy which is originally responsible for promoting and disseminating the rights of individuals to information, and in turn resolves on the refusal of applications for access to information, and protects the personal data held

by the departments and entities of the state. As from 6 July 2010, it is also the authority responsible for ensuring the protection of personal data held by individuals.

The internal regulations of the IFAI were amended on 28 April 2011, in order to set up the Data Protection Ministry, which is made up of 14 directorates, and is granted power in the field of personal data protection.

2.2 Powers

The IFAI has the following powers:

- to coordinate and oversee the development of regulatory projects in the field of personal data protection;
- to coordinate and oversee the development of views on the interpretation for administrative purposes of the LPPD;
- to coordinate and monitor the reception, process and determination of procedures for the protection of rights;
- to carry out actions to foster a reconciliation between the data subject and the data controller, and if necessary provide the respective agreement;
- to coordinate and supervise the inspections to monitor compliance with the LPPD;
- to supervise, coordinate and substantiate the procedures for imposing sanctions;
- to issue the relevant decision and notify the parties;
- to coordinate the dissemination and publication of studies on standards and better international practice in the field of information security with relevance to the nature of personal data;
- to supervise the purposes of treatment, and technical and economic capabilities of the data controller;
- to monitor and provide follow-up to the implementation of resolutions on the protection of data issued by the IFAI;
- in cooperation with the Ministry of Economy, to accredit third party certifiers to harmonise the treatment of personal data in accordance with the provisions of applicable law;
- to prepare reports to authorities on the sanctions imposed on perpetrators or violators of the LPPD, and inform the legal department of the conduct alleged to constitute an offence for any legal purposes required; and
- to collaborate with other domestic and foreign supervision and organisation authorities, on data protection, among other things.

It is noteworthy that in addition to the IFAI, which will be the executing authority for the LPPD, the law also empowers the Ministry of Economy to disseminate knowledge of the obligations relating to the protection of data between the local and international private initiatives that have commercial activity in Mexican territory. Additionally, it was also granted authority to promote better business practice regarding the protection of personal data as an input for the digital economy and aspects of self-regulation in the industry.

Likewise, the Ministry of Economy has the authority to issue regulations regarding automated trade databases or those forming part of a process of automation, as well as:

- to disseminate knowledge in the commercial field;
- to promote fair trade practice in the field of protection of personal data;
- to set guidelines to define the content and scope of privacy alerts in support of the IFAI;
- to issue, within the scope of its competence, administrative provisions of a general nature in support of the IFAI;
- to set up the parameters necessary for the proper development of mechanisms and measures of self-regulation and promotion of Mexican Standards or Official Mexican Standards in support of the IFAI;
- to record consumer personal data and verify their operation;
- to come to agreements with chambers of commerce, associations and business organisations in general on the protection of personal data;
- to design and implement policies, and to coordinate the preparation of studies for the modernisation and efficient operation of e-commerce, and to promote the development of the digital economy and information technologies in the protection of personal data;
- to attend national and international business forums or congresses on the protection of personal data, or those events of a commercial nature; and
- to support the realisation and implementation of events which contribute to the dissemination of personal data protection.

2.3 Priorities

The LPPD sets out a timetable and one of the most important deadlines is 6 January 2012, the date on which data subjects will be able to exercise their rights to access, rectify, cancel and oppose, as well as initiate the procedure for the protection of rights before the IFAI.

The IFAI has stated on several occasions that its priority intention for the year 2011 is to spread throughout all the mass media the scope of the LPPD, since it is not its intention to initiate the law in its immediate form with verifications or infringement procedures, but to inform the public of the existence of the law and the need for its observance, with the objective of creating a real culture in the field of protection of personal data.

3. LEGAL BASIS FOR DATA PROCESSING

The LPPD in Mexico allows the processing of personal data provided that it is made in a legitimate, controlled and oriented manner ensuring the privacy of the data subject's personal data, and the right to informational self-determination.

In terms of sensitive data, creating databases of this nature is permitted provided that their existence can be justified in regard to the aim pursued.

3.1 Consent

3.1.1 Definition

Consent is the main basis for being able to use the personal data of individuals in Mexico. In accordance with the LPPD, 'consent' is the 'manifestation of the will by the data subject through which such data are processed', and any treatment is submitted to the consent of the data subject, except as otherwise provided in the Law.

3.1.2 Form

Consent is given after a privacy notice has been made available to the data subject and the latter does not express any kind of opposition. In the case of sensitive or financial data, the law requires that the consent be granted explicitly (written, by electronic means or any other technology, or by unequivocal sign).

3.1.3 In an employment relationship

The new LPPD does not set out any approach in regard to the validity of consent from an employee. The only requirement is to put a proper privacy notice at the disposal of the employee, to obtain explicit consent where data of sensitive or financial nature are collected, and to comply with the other general provisions of the LPPD itself.

3.2 Other legal grounds for data processing

The LPPD provides exemptions from the requirement to obtain consent to the processing of personal data in the following instances:

- if it is provided under any law;
- if the data are accessible through public sources;
- subject to a prior process of dissociation;
- if it is necessary to comply with obligations arising from a legal relationship between the data subject and the data controller;
- if there is an emergency situation that may potentially harm an individual's well-being or property;
- if it is essential for medical care, while the data subject is unable to give consent and such data process is carried out by a person subject to the obligation of professional secrecy or equivalent; or
- if an authority has handed down a decision which so requires.

Likewise, in the field of personal data transfers, local or foreign transfers will not be subject to the LPPD when:

- the transfer is provided by a law or treaty to which Mexico is a party;
- the transfer is necessary for preventive medical purposes and/or medical diagnosis;
- the transfer is made to holding companies, subsidiaries or affiliates under the common control of the person in charge, or to a parent company or any society of the same group which operates following the same procedures and internal policies;
- the transfer is necessary by virtue of a current or future contract in the interest of the data subject, by the data controller and a third party;
- the transfer is necessary or legally required to safeguard the public interest, or to provide and administer justice;

- the transfer is required for the recognition, exercise or defence of a right in a judicial process;
- the transfer is required for the maintenance of, or in compliance with, a legal relationship between the data controller and the data subject.

3.3 Direct marketing and cookies

With regard to direct marketing and cookies, the LPPD does not set out anything in particular, but it is expected that the Regulations will contain provisions relating to both issues. At the moment, the use of marketing systems is subject to consent that must be sought by means of the privacy notice.

On the other hand, in the field of direct marketing, the Federal Law on Consumer Protection establishes that the supplier is obliged to use all information provided by the consumer confidentially. Moreover, the supplier must abstain from using advertising or sales strategies that do not provide clear and sufficient information about the services offered, particularly in the case of marketing aimed at vulnerable target markets, such as children, the elderly and the sick (special mechanisms should be incorporated to advise that the information is not suitable for this sector of the population).

The Authority has stated that it will study the issue of cookies in the future. Recently, the IFAI and the Ministry of Economy together issued a practical guide to generating a privacy notice, and within the models suggested in the guide, the need to make a reference to the 'cookies' and 'beacons' used in the privacy notice is mentioned, as well as the kind of information that is collected through these files. It is important to mention that the IFAI will have the power to issue criteria for the interpretation of the law, which may be taken into consideration by individuals in their implementation of the law.

3.4 Data quality requirements

The law provides eight principles that must be honored by the data controller. The principles for the protection of personal data are: legality (the data must be obtained in accordance to the law); consent (the data protection right consists of the power of the data subject to control the data); information (the right to be aware of the existence and details of a process by means of a privacy notice); quality (the data are expected to reflect the exact information processed); purpose (the process must be carried out in a determined, explicit and legitimate manner in regard to the data subject activity); loyalty (the data controller shall look after the fulfillment of these principles); proportionality (the data controller is expected to process only the strictly necessary data and make use of the minimum information for that purpose); and responsibility (the warranty provided from the data subject to the data controller, who should take all necessary measures to make sure the data are processed according to his/her will) for the treatment of personal data.

3.5 Outsourcing

Personal data can be transmitted by the data controller to third parties other than the data processor in Mexico or abroad as long as these third parties have been provided with a privacy notice, and have been informed about the purpose for which the data subject gave his consent. Also, the process should be undertaken according to the privacy notice, which must contain a clause indicating whether the data subject accepts the transfer of data or not, and the third party recipient shall assume the obligations that correspond to the person who transferred the data.

3.6 Email, internet and video monitoring

3.6.1 General rules

The LPPD contains no particular provisions with regard to either surveillance cameras, email or the internet. Nevertheless, should personal data be collected through email or websites, it must be obtained using simplified privacy notices necessary to indicate to the owner of the personal data how to access the privacy notice, and thus assert his right to access, rectify, cancel and oppose the data, as well as the name and address of the data controller's personal data department.

3.6.2 Employment relationship

The LPPD in Mexico contains no provisions on practices involving employee monitoring.

4. INFORMATION OBLIGATIONS

4.1 Who

The data controller has the obligation to inform the data subject of the treatment or processing which will be given to his or her data, and must set a deadline for such process.

4.2 What

The following information must be provided through the privacy notice:

- the identity and address of the person in charge of collecting it;
- the aim of the data processing;
- the options and means that the data controller offers to the data subjects in order to limit the use or disclosure of the data;
- the way to practice the rights of access, rectification, cancellation or opposition in accordance with the law;
- where appropriate, data transfers made;
- the procedure and way in which the data controller shall communicate to the data subject any changes to the privacy noticing accordance with the law.

As for sensitive data, the privacy notice must clearly point out that it contains such data.

4.3 Exceptions

Not applicable.

4.4 When

The privacy notice should be made available to the data subjects through printed, digital, visual or audio formats, or any other technology, as follows:

- When personal data have been collected personally from the data subject, a privacy notice must be provided clearly and efficiently at the time the data are collected, through the form that they are sought, unless the notice had been supplied beforehand.
- When personal data are obtained directly from the data subject by any electronic, optical, sound or visual means, or using any other technology, the data controller must immediately provide the data subject with an identity and address, as well as the purpose of the process and the procedure that the data subject must follow to find the complete text of the privacy notice.

4.5 How

The LPPD provides that the information should be made available to the data subjects through printed, digital, visual or audio format, or using any other technology.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Data subjects have the right to access the personal data that are being dealt with by the data controller for the data, as well as to know the scope of such treatment or process, using the privacy notice.

Any person who has provided his or her personal data to a data controller may access such personal data by means of a request for access, which must at least contain the following:

(i) the name of the data subject, the address or any other form of location to send a response;
(ii) documents providing an identity or that of his or her legal representative;
(iii) a clear and precise description of the personal data regarding which he seeks to exercise any right; and
(iv) anything else that facilitates the location of the data.

In particular, in the case of requests for access to personal data, the delivery of it shall be provided upon reliably certifying the identity of the applicant or the legal representative, and shall be deemed fulfilled when it is made available to the data subject, either through the issuance of simple copies, electronic documents or any other means as determined by the data subject in the privacy notice.

5.1.2 Exceptions

There is no provision under which to deny the right of access to data subjects. In the event that the data subject requests access to data to a person who is incorrectly presumed to be the data controller, it will suffice to tell the data subject by any means referred to in the preceding

paragraph, in order to fulfil the request.

The LPPD states that the data controller may deny access to personal data or refuse to correct, cancel or oppose it, only under the following circumstances:

- when the applicant is not the data subject, or the legal representative is not duly accredited to make the request;
- when the personal data from the applicant cannot be found in the database;
- when the rights of a third party are infringed;
- when there is a legal impediment or a resolution from a competent authority which restricts access to the personal data or does not allow rectification, cancellation or opposition to it; and
- when the rectification, cancellation or opposition has been performed already.

The refusal referred to above may be partial.

5.1.3 Deadline

There is no particular deadline as to when a data subject can access his personal data.

This right, as well as any of those recognised under Mexican law (access, rectification, cancellation and opposition (ARCO)) must be handled by the Department of Protection of Personal Data (Chief Privacy Officer of the data controller).

The data controller must provide a response within a period of 20 days from the date of receipt of the request. Additionally, in the case of a cancellation request, the data controller has another 15-day period to delete the part of the data which the data subject has requested. These time limits may be extended once, for an equal period of 20 or 15 days, provided it is justified in each particular case.

5.1.4 Charges

In Mexico, the delivery of information when exercising the right to access must be free of charge. The data subject should only cover the substantiated costs of shipping or the reproduction of copies, or other formats.

However, if the same person makes another request within 12 months, the costs will not be greater than $179.46 Mexican pesos (equivalent to three days of minimum wage in Distrito Federal (Mexico City)), unless there are substantial changes to the privacy notice that necessitate further consultations.

5.2 Rectification

5.2.1 Right

It is the right of the data subject to modify any data which are imprecise or incomplete.

5.2.2 Exceptions

There are no exceptions to the right of rectify. The LPPD only demands that,

for the right to rectification, the data subject shall indicate, in addition to the information listed in section 5.1.1, the modifications to be made and provide the documents supporting the request.

5.2.3 Deadline

There is no deadline for performing the right of rectification. The times for the controller to respond to this right are the same as in section 5.1.3.

5.2.4 Charges

The data subject may not be charged for exercising the right of rectification.

5.3 Erasure

5.3.1 Right

Mexican law does not establish an express right to erasure. This right can be equated with the right of cancellation referred to by the LPPD. The right of 'cancellation' is the right of the data subject which gives rise to completely delete or to delete any data found to be inadequate or excessive in relation its treatment.

5.3.2 Exceptions

See section 5.1.2.

5.3.3 Deadline

There is no deadline for performing the right of cancellation.

5.3.4 Charges

The data subject may not be charged for exercising the right to cancellation. The times for the controller to respond to this right are the same as in section 5.1.3.

5.4 Blocking

The right to block does not apply expressly under Mexican law. However, it could be equated with the right to object (see section 5.5 below).

5.5 Objection

5.5.1 Right

The LPPD calls this the right of opposition. This right refers to the prerogative of the data subject to oppose the using of his or her personal data for a specific purpose.

The exercise of this right must be based on the particularity of the situation itself, or of the person concerned, justifying that while the treatment is fully lawful, it is still necessary to oppose it in order to avoid prejudice.

5.5.2 Exceptions

See section 5.1.2.

5.5.3 Deadline
There is no deadline for performing the right of opposition. The times for the controller to respond to this right are the same as in section 5.1.3.

5.5.4 Charges
The data subject may not be charged for exercising the right to opposition.

5.6 Automated individual decisions
Not applicable.

5.7 Other rights
Not applicable.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
In principle, the LPPD does not require notification of the creation, processing or transfer of databases. When it comes to databases of sensitive data, their creation must be justified, but notification is not necessary. The justification will be reviewed by the Authority at the time of an official inspection.

However, binding schemes of self-regulation such as codes of ethics or fair professional practice, trust or confidence or other mechanisms aimed at establishing specific rules or standards to harmonise data processing carried out by the adherents to them and facilitate the exercise of the rights of data subjects, must be notified simultaneously to the relevant sectorial authorities and the IFAI.

At the time of writing, specifications about the law regulations on self-regulation have not been published. Therefore, there currently is no additional information about this subject.

6.2 Authorisation requirements
6.2.1 Who
The data controller is responsible for requesting authorisation.

6.2.2 What
When it is impossible to inform the data subject of the privacy notice (see section 4 above), or if it involves a disproportionate effort due to the number of data subjects or the age of the data, the data controller may implement compensatory measures, such as mass mail, periodical publishing or internet publishing. The compensatory measure must be approved by the Authority.

6.2.3 Exceptions
Until now, while the LPPD Regulations are still under public consultation, there are no specific exceptions with regard to the authorisation requirement.

6.2.4 When
Any compensatory measure must be approved by the IFAI preceding its

implementation. The authorisation of the compensatory measure does not have to be renewed.

6.2.5 How

The request for authorisation has to be submitted to the IFAI in writing. The LPPD does not provide for any details as to the procedure to obtain authorisation from the IFAI, nor for any standard application. These applications have been submitted in writing, targeted at the IFAI, which has provided a response in the same way. The authorisation does not have a fixed term. No statistics have so far been issued by the Authority to indicate the number of compensatory measure applications submitted to date.

6.2.6 Authorisation fees

The application for authorisation for compensatory measures is free of charge.

6.3 Other registration requirements

Not applicable.

6.4 Register

Not applicable.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

In Mexico, it is the duty of all data controllers to designate another person (or a personal data department) who has an obligation to: (i) respond to requests of data subjects whose personal data are treated by the company, regarding the exercise of their rights; and (ii) promote the protection of personal data within the organisation.

The requirement to have a department for personal data protection began on 6 July 2011, for all those companies or individuals who process personal data, and it will depend on the size of the company and the nature of the data to be addressed as to whether a person is commissioned for this activity, or a specific department is created to fulfil this function.

7.2 Tasks and powers

The LPPD does not contain the obligations or rights for the department of protection of personal data or a specific protocol for appointment. However, the IFAI and the Ministry of Economy have issued a series of non-binding recommendations regarding the allocation of the person or department of personal data.

These recommendations are aimed at describing the obligations placed on the head of the department of protection of personal data.

Where requests are received from data subjects in relation to exercising rights over their data, the person or department should: (i) establish and administer procedures for receiving, processing, monitoring and timely treatment of requests for the exercise of the rights of access, rectification,

cancellation and opposition, as well as examining complaints or requests from data subjects relating to policies and/or practices for protecting personal data developed by the organisation; and (ii) monitor the progress or legislative amendments on privacy and protection of personal data that could impact the guiding ideas and actions on this issue within the organisation, making the necessary adjustments.

With regard to promoting the protection of personal data within the organisation, it is recommended to:

- design and implement a policy and/or practices on personal data protection within the organisation, or, adapt and improve already existing practices within the framework of the law;
- align policy and/or practices (including its objectives, strategic actions, courses of action, allocation of roles and responsibilities in general or specific, procedures and the timing of implementation) with the internal processes of the organisation that require or make use of personal information;
- develop a mechanism to assess the efficiency and effectiveness of the policy and/or practices;
- monitor and evaluate the internal processes of the organisation associated with the procurement, use, exploitation, conservation, use, cancellation and transfer of personal data, in order to ensure that the information is protected, treated in accordance with the principles of the law, and respected;
- collaborate and coordinate activities with other areas of the organisation, such as legal, technology, systems, information security, marketing, customer support, human resources, etc with the purpose of ensuring due compliance with the policies and/or privacy practices in internal processes, formats, notices, resources and efforts that are carried out;
- ensure that the policy and/or practices concerning the protection of personal data comply with the law and any applicable regulations;
- disseminate and communicate the policy and/or practices for the protection of personal data implemented within the organisation, as well as provide adequate staff training;
- promote a culture of protection of personal data aimed at improving the level of awareness of the staff and third parties involved, such as managers, in the processing of personal data;
- follow up compliance with the policy and/or practices for the protection of personal data by subsidiaries or affiliates under common control of the organisation, or any operating society from the same group where the practices may be applied;
- identify and implement better practices regarding the protection of personal data;
- promote the adoption of self-regulating schemes;
- be the representative of the organisation in terms of the protection of personal data before others.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The LPPD contains a specific chapter on data transfer, which states that when a data controller intends to transfer personal data to domestic or foreign third parties other than the data controller (ie, the natural or legal person who alone or jointly processes personal data on behalf of the individual responsible) he must communicate or extend the privacy notice to the third parties, as well as the purposes for which the data subject submitted his data.

8.2 Legal basis for international data transfers

The processing of the data will be performed in accordance with the privacy notice, which should include a clause which indicates whether the data subject agrees or not to the transfer of his or her data. Similarly, the third party recipient should assume the same obligations that correspond with the data controller for that transferred data.

8.2.1 Data transfer agreements

The main content of a transfer agreement consists of requiring the third party recipient of the personal data to assume the same obligations as the person that transferred the data, as well as the demonstration of security measures similar to those applied by the data controller. There is as yet no standard format for a transfer agreement and the form of implementation is still evolving.

8.2.2 Binding corporate rules

There are no formal rules relating to binding corporate rules on transfer of personal data. However, the LPPD provides that natural or legal persons may agree between them or with civil or governmental, national or foreign societies, binding self-regulatory schemes to complement the provisions of the law. In addition, it is required that these self-regulatory schemes contain mechanisms to measure their effectiveness for the protection of data, as well as the consequences and effective corrective measures in the case of infringement.

These models of self-regulation may translate into codes of conduct or fair professional practice, or other mechanisms which set rules or specific standards to harmonise the processing of data carried out by data processors and to facilitate the exercise of the rights of data subjects.

8.2.3 Safe Harbour

There is no need for authorisation where personal data are transferred to an organisation that is certified under the US Safe Harbour scheme and the data transfer falls within the scope of that certification. Nevertheless, given that an international transfer to a third party is being carried out, such transfer must be referred to in the privacy notice.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

In accordance with the LPPD, the data controller or third parties involved in any stage of the processing of personal data must maintain confidentiality at all times. It is important to mention that this obligation shall continue even after the relationship with the data subject or data controller has finished.

9.2 Security requirements

In Mexico, every data controller must establish and maintain security measures of three types: (i) administrative; (ii) technical; and (iii) physical. These measures must protect personal data against damage, loss, alteration, destruction or unauthorised use, disclosure or processing.

Additionally, the LPPD compels data controllers not to take lower security measures than those which exist for the handling of information, taking into account the existing risk, the potential implications for the data subjects, the sensitivity of the data and technological development.

9.3 Data security breach notification obligation

9.3.1 Who

Under the LPPD it is for data controllers to notify data subjects of security breaches.

9.3.2 What

Breaches of security that occurred at any stage of the processing which significantly affect the patrimonial or moral rights of the data subjects must be notified. It is expected that this information will be further widened in the Regulations.

9.3.3 To whom

Breaches must be notified to data subjects.

9.3.4 When

Notification must take place immediately upon detecting a breach in security measures, so that the data subjects can take relevant action to protect their rights.

9.3.5 How

So far, there are no specific rules as to how a breach should be notified to data subjects.

9.3.6 Sanctions for non-compliance

Article 63 fraction XI of the LPPD establishes infringement as 'breach of the security of databases, local, programs or equipment when imputable to the data controller.' This infringement is sanctioned with a fine ranging between $11,964.00 pesos (US$957.12), and $19,142,400.00 pesos (US$1,531,392.00).

The power to impose these sanctions will be granted to the IFAI once the corresponding Regulations have been issued from 6 January 2012.

9.4 Data protection impact assessments and audits

So far, data protection impact assessments and audits are only recommended by the Authority, but there is no obligation to implement them, nor have specific rules been issued in this regard. In practice they are highly recommended in order to consider an organisation as well positioned in terms of protection of personal data, as well as to establish the security measures consistent with the treatment and nature of processed personal data.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The IFAI has the power of verification on its own initiative for the purpose of reviewing compliance with the LPPD and the Regulations arising from it. This verification can be carried out on its own motion (automatic) or upon request.

Automatic verification occurs when there is non-compliance with procedures for the protection of rights, or when violations of the law are presumed. It is important to mention that during the verification procedure the IFAI will have access to any information and documentation deemed necessary, which public servers are obliged to keep confidential. Form, terms and deadlines to operate this procedure will be developed by the Regulations.

Furthermore, when the act derives from a procedure for the protection of rights, the IFAI may impose as a first step, a warning to the data controller to carry out the actions requested by the data subject, in terms of compliance with the requests for ARCO rights to the processing of personal data.

Given it is a new law, no actions have been initiated by the IFAI yet.

10.2 Sanctions

The LPPD provides for two criminal offences and 19 administrative offences.

In the field of criminal offences, the two scenarios are as follows: (i) three months to three years imprisonment where the person authorised to process personal data causes a breach of security related to the databases in his or her custody for profit; and (ii) imprisonment from six months to five years for seeking undue profit by processing personal data deceptively, or taking advantage of an error on the part of the data subject or the authorised data processor. In the case of sensitive personal data, these penalties will be doubled.

In administrative matters, the sanctions for infringements are as listed below:

- A warning to the data controller to carry out the actions requested by the data subject, in the case of ARCO rights requirements.
- A fine from $5,982.00 pesos (US$478.56.00) to $9,571,200.00 pesos (US$765,696.00), in the following cases of infringement, regardless of the first sanction in the preceding paragraph. These cases are:
  (i) acting with negligence or wilful misconduct in handling and responding to requests for access, rectification, cancellation or opposition of personal data;
  (ii) fraudulently declaring the non-existence of personal data when

there is total or partial data in the databases of the data controller;
(iii) treating personal data contrary to the principles set out in the LPPD;
(iv) omitting any or all the elements referred to in Article 16 of the LPPD in the privacy notice;
(v) maintaining inaccurate personal data when imputable to the data controller, or not making the legal and appropriate corrections or cancellations when affecting the rights of the data subjects; and
(vi) failure to comply with the warning referred to in section I of Article 64.

- A fine ranging from $11,964.00 pesos (US$957.12.00) to $19,142,400.00 pesos (US$1,531,392.00), in the following cases:
(vii) breaching the duty of confidentiality laid down in article 21 of this Act;
(viii) substantially altering the original purpose of data processing, without observing the provisions of Article 12;
(ix) transferring data to third parties without informing them of the limitations provided in the privacy notice disclosed by the data subject;
(x) violating the security of local databases or equipment programs when imputable to the data controller;
(xi) carrying out the transfer of personal data other than the cases permitted by the Law;
(xii) whenever required, collecting or transferring personal information without the express consent of the data subject;
(xiii) obstructing acts of verification of the authority;
(xiv) collecting data in a misleading and fraudulent manner;
(xv) continuing the illegitimate use of personal data after either the IFAI or the data subject have requested use to stop;
(xvi) treating personal data in such a way that affects or prevents the exercise of the rights of access, rectification, cancellation and opposition established in Article 16 of the Political Constitution of Mexico;
(xvii) creating databases in contravention to the provisions of Article 9, paragraph II of LPPD, and
(xviii) failure from the data controller to comply with the obligations set out in the terms of the provisions in the LPPD.

- In the event that the abovementioned offences persist, an additional fine will be imposed, ranging from $5,982.00 pesos (US$478.56.00) to $19,142,400.00 pesos (US$1,531,392.00). If the offences were committed when processing sensitive data, the penalties may increase up by two times the established amounts.

10.3 Examples of recent enforcement of data protection rules

There are no examples yet.

10.4 Judicial remedies

In the event that the IFAI imposes an administrative sanction on a data

controller, the latter may challenge the resolution through a trial for nullity (*Juicio de Nulidad*) before the Federal Court of Fiscal and Administrative Justice, which is made up of chambers, with three judges per chamber.

In the event that the court confirms the resolution of the IFAI, the data controller can gain access to a '*Juicio de Amparo*' (Constitutional trial) before the Collegiate Circuit Courts in Administrative Matters (*Tribunales Colegiados de Circuito en Materia Administrativa*), which are also composed of three judges who analyse issues of unconstitutionality derived from acts of federal authority.

In the event that the data subject wishes to put his rights into action before the data controller, he must make a request before the chief privacy officer of the data controller, who shall have the responsibility to establish a procedure in order to fulfill these rights. Once the request has been made, the data controller will have to provide a response in the times referred to in section 5.1.3. If the data controller does not provide a timely response or the data subject does not agree with such response, he or she will be able to file a procedure for the protection of rights before the IFAI, which will require the data controller to comply in accordance with the law.

10.5 Class actions

Class actions are uncommon in Mexico. An amendment to Article 17(3) of the Political Constitution of the Mexican United States was published on 29 July 2010. This reform gives power to Congress to issue laws governing class actions in Mexico. As a result, on 30 August 2011, the Official Journal published modifications to various federal laws that allow collective action or class actions in Mexico, which will enter into force six months after their publication. In principle, these actions can only be pursued in relation to the consumption of goods, public or private services and the environment. It cannot yet be foreseen whether they will become applicable to actions relating to data protection.

10.6 Liability

The fines imposed by the LPPD must be collected and are the property of the Mexican State. However, the law also establishes that sanctions shall be imposed without prejudice to civil or criminal liability, which allow the possibility that the data subjects can claim in different instances for damage caused by the violation of their personal data based on civil law.

The LPPD already holds a complete structure for efficient performance in Mexico. By the delivery date of this work, the IFAI will have been provided with enough economic resources from the Federal Government, and hired and trained over 70 people who will be in charge of applying this law correctly. Furthermore, the IFAI is planning to sign agreements to collaborate with other authorities in order to extend to them its faculties so that it can cover the whole of Mexico and develop the systems and procedures necessary for its efficient performance.

Netherlands

Vondst Advocaten Polo van der Putt & Eva de Vries

1. LEGISLATION

1.1 Name/title of the law

The Data Protection Directive 95/46/EC has been implemented in the Data Protection Act of 6 July 2000 (*Wet bescherming persoonsgegevens*) (Data Protection Act) and a couple of further decrees. Of special significance is the Exemption Decree Data Protection Act of 7 May 2001 (*Vrijstellingsbesluit Wbp*) (Exemption Decree), which regulates certain exemptions from the notification obligation.

As to the use of personal data for marketing by phone and electronic mail, the Telecommunications Act (*Telecommunicatiewet*) is applicable.

The collection and processing of personal data is also regulated by various more specific laws and regulations, such as the Police Data Act (*Wet politiegegevens*), the Municipal Personal Records Act (*Wet gemeentelijke basisadministratie*) and the Works Council Act (*Wet op de ondernemingsraden*).

Collection and processing of personal data should be in accordance with the constitutional (and international conventional) right of privacy. Violation of this right of privacy can be tortious.

1.2 Pending legislation

Currently an amendment to the Data Protection Act is being discussed in the Senate (the Second Chamber of parliament has already approved the amendment). The amendment aims to decrease the administrative burden caused by the Act. In short it intends to: (i) simplify the information obligations with respect to direct mail; (ii) abolish the permit requirement in relation to international data transfers if use is made of one of the European Commission's standard contractual clauses; and (iii) to improve and simplify the wording of the Act.

In addition, there is a discussion in the parliament with regard to the notification of data breaches, the extension of the Data Protection Commission's power to levy fines, the information to consumers with regard to the term of data storage, a privacy impact assessment for future legislation and the creation of a privacy help desk.

Recently, a proposal to amend the Telecommunications Act has been published in order to implement the amendments to the ePrivacy Directive, brought about by Directive 2009/136/EC.

1.3 Scope of the law

1.3.1 The main players

- The 'data subject' is the person to whom personal data relate.
- The 'data controller' is the natural person, legal person, administrative

body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal data.
- The 'data processor' means the person or body which processes personal data for the data controller, without coming under the direct authority of that party.
- A 'third party' is defined as any party other than the data subject, the data controller, the data processor, or any person under the direct authority of the data controller or the data processor, who is authorised to process personal data.
- The 'recipient' is the party to whom the personal data are provided.

1.3.2 Types of data

The Data Protection Act relates to personal data, defined as '*any information relating to an identified or identifiable natural person*'. According to the Data Protection Commission, anonymous and coded data are not considered personal data, provided that the persons concerned cannot reasonably be identified. Such is deemed to be the case when the person processing the data cannot identify the natural persons concerned without using exceptional means or using an unreasonable amount of time to do so.

A stricter privacy regime applies to certain specific categories of data, often called 'sensitive data'. The following data are recognised as sensitive data: personal data concerning a person's religion or philosophy of life; race; political persuasion; health and sexual life; or personal data concerning trade union membership; criminal behaviour; or unlawful or objectionable conduct connected with a ban imposed on conduct.

1.3.3 Types of acts/operations

The Data Protection Act applies to the fully or partly automated processing of personal data and the non-automated processing of personal data entered or intended to be entered into a file. The term 'processing' should be interpreted broadly, and includes any operation or any set of operations concerning personal data, including in any case the collection; recording; organisation; storage; updating or modification; retrieval; consultation; use; dissemination by means of transmission; distribution or making available in any other form; merging; linking; as well as blocking; erasure or destruction of data.

A 'file' is defined as any structured set of personal data, regardless of whether or not the data set is centralised or dispersed along functional or geographical lines, accessible according to specific criteria and relates to different persons.

1.3.4 Exceptions

Activities that fall outside the scope of the Data Protection Act are the following acts of data processing:
- data processing in the course of a purely personal or household activity;
- data processing by or on behalf of the intelligence or security services referred to in the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten*);
- data processing for the purposes of implementing the police tasks defined

in Article 2 of the Police Act 1993 (Politiewet 1993);
- data processing governed by or under the Municipal Personal Records Act;
- data processing for the purposes of implementing the Judicial Documentation Act (*Wet justitiële documentatie*); and
- data processing for the purposes of implementing the Electoral Provisions Act (*Kieswet*).

1.3.5 Geographical scope of application

The Data Protection Act applies to the processing of personal data by a data controller that:
- has an establishment in the Netherlands; or
- is not established in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands, unless these means are used only for forwarding personal data. In this case, the data controller must designate a person or body in the Netherlands to act on its behalf in accordance with the provisions of the Data Protection Act.

In line with the opinion of the Article 29 Working Party, in short the Data Protection Commission takes the position that the Data Protection Act only applies when a Dutch entity in effect controls a certain process. If data are factually processed by an office in the Netherlands of a foreign company, but a foreign establishment of that company in effect controls the processing, the Data Protection Act would not apply. This view has been disputed in legal literature.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Data Protection Commission (*College Bescherming Persoonsgegevens*).
Juliana van Stolberglaan 4-10
2595 CL DEN HAAG
PO Box 93374
2509 AJ DEN HAAG
Netherlands
Telephone:
General: +31 (0)70-8888 500
Consultation 9:30-12:30: 0900-2001 201
Press: +31 (0)70-8888 555
F: *+31 (0)70-8888 501*
E: info@cbpweb.nl
W: *www.cbpweb.nl*

2.1 Role and tasks

The task of the Data Protection Commission is to oversee the processing of personal data in accordance with the provisions laid down by and under Data Protection Act. The Data Protection Commission also oversees the processing

of personal data in the Netherlands, where the processing takes place in accordance with the laws of another country of the European Union. Furthermore, the Data Protection Commission undertakes the following tasks:

- advice on legislation;
- assessment of codes and regulations;
- handling of notifications and conducting prior investigations of certain processing of personal data;
- education;
- advising the Minister of Justice on permits for transferring personal data to third countries.

Currently, the Data Protection Commission has approximately 70 employees.

2.2 Powers

Powers of the Data Protection Commission in practice include *ex officio* investigations and enforcement of the Data Protection Act, *inter alia* by making the names of the breaching data controllers public, taking administrative enforcement actions and by imposing administrative fines. The Data Protection Commission may investigate at its own discretion or on request by an interested party the manner in which the provisions laid down by or under the Data Protection Act are being applied with respect to the processing of personal data.

The appointed officers of the Data Protection Commission are authorised to enter a residence without the consent of the resident. In addition, each officer has the right to enter any place, and may demand information and make copies of data and papers. The Data Protection Commission has the right to research vehicles, to take samples and to open packaging.

2.3 Priorities

In general, the Data Protection Commission focuses on material privacy breaches. Priority is given to violations that have a big impact on privacy or on minor violations affecting many data subjects. In practice, companies active in a regular course of trade, will not quickly be subject to an investigation. Besides, even if the Data Protection Commission finds minor violations, it often will only give a warning, provided the violator can demonstrate good faith and is prepared to improve, eg, by implementing new privacy procedures.

From time to time the Data Protection Commission announces specific areas that it will focus on. Most recently the Commission has announced that it will, among others, focus on the following topics:

- processing of geolocation data;
- sharing of data and profiling on the internet;
- data breaches;
- systems tracking citizens in social security matters;
- public transport information;
- investigation on data processing in relation to Europol, Schengen and the Working Party on Police and Justice;
- supervision of the processing of (sensitive) data by government and

schools; and
- supervision of the processing of police data.

The Data Protection Commission works closely with other European data protection authorities in defining a joint strategy. It has been active in the debate in the EU on the future of the Directive and reviewing and discussing so-called binding corporate rules regarding the transfer of personal data by multinationals (see section 8.2.2 below).

3. LEGAL BASIS FOR DATA PROCESSING

3.4 Consent

3.4.1 Definition

'Consent' of the data subject means '*any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal data relating to them*'. In the explanatory notes the Data Protection Commission has further substantiated the notion of consent. Specific and informed means that the scope of the consent is precisely defined and consistent with what the person in the circumstances expected and could see. This should enable the data subject to balance his interests in protecting his privacy on the one hand and the benefits of providing personal data on the other hand.

3.4.2 Form

No specific form is prescribed for consent.

3.4.3 In an employment relationship

According to the Data Protection Commission, in general one may not assume that valid consent can be given in an employment relationship, because of the relationship of dependence. An example of data processing for which, according to the Commission, consent of an employee is necessary and possible, is the use of photos for an internal online 'who's who' directory.

3.5 Other legal grounds for data processing

Apart from obtaining consent, personal (non-sensitive) data can be processed based on any of the following grounds:
- the processing is necessary for the performance of a contract to which the data subject is a party;
- the processing is necessary for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract;
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject;
- the processing is necessary in order to protect a vital interest of the data subject;
- the processing is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the data are provided; or
- the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject prevail.

Apart from obtaining consent, sensitive data may only be processed under certain conditions, depending on the type and use of the data. For instance, health data may be processed in the course of medical treatment and criminal data in the course of criminal prosecution. Information on ethnic origin may be processed if it is necessary and relevant for identification or for affirmative action. Only trade unions may process trade union membership information (unless consent has been obtained).

3.6 Direct marketing and cookies

General rules for direct marketing may be found in the Data Protection Act. Under these rules the data subject has a right to oppose the processing of its data for direct marketing purposes, without any justification being necessary. Furthermore the data subject must be informed of his right to oppose in any direct marketing communication.

As to direct marketing by means of telecommunication, the Telecommunications Act provides for detailed regulation and provides for an (opt-in) regime (which basically requires consent) for marketing via SMS and email with an exemption for customers of the company (under certain conditions). As to promotional phone calls, an opt-out regime applies.

Specific rules regarding cookies are detailed in the universal service and end users interests decree (*'Besluit universele dienstverlening en eindgebruikersbelangen'*), a further regulation to the Telecommunications Act. According to this decree, website owners should inform data subjects of the use of cookies, the fact that cookies may be rejected and how this can be done. Data subjects should also be given the possibility to reject cookies. Currently not many websites meet these requirements. In general it is believed that the possibility for internet users to set browser cookie settings offers sufficient protection. There is hardly any enforcement action by the regulators.

Further to the amended ePrivacy Directive, an amendment to the Telecommunications Act was proposed to the Senate in June 2011. Further to this proposal, the visitor to the website has to give its explicit consent for the use of cookies. This would mean that a specific browser setting is no longer sufficient. An exemption is made for cookies that are solely placed to enable certain technical functionalities for browsing the website. If this proposal is passed, it is expected to enter into force in the first half of 2012.

3.7 Data quality requirements

Personal data may only be processed where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive. In this respect, the data controller should take the necessary steps to ensure that personal data are correct and accurate. In addition, personal data may not be retained longer than necessary.

3.8 Outsourcing

Where the data are processed by a third party processor, the data controller must ensure that the data processor provides adequate guarantees for security. The parties have to enter into a processing agreement in writing. In

such agreement, the data controller has to stipulate that the data processor processes the personal data in compliance with the relevant security obligations.

Apart from that, there are no additional specific regulations for outsourcing. However, in June 2011 the Data Protection Commission expressed its viewpoints on outsourcing. Among others it has taken the following position:

- The outsourcer always remains responsible for the personal data that are outsourced.
- The outsourcing service provider normally will be a data processor, but may be a data controller, depending on the level of control it can exercise.
- The data subjects should be informed of outsourcing involving their data.
- Data subjects should be informed of the use of possible sub-processors and be given the right to object to them.
- The outsourcer should have the contractual right to audit compliance of the security obligations by the outsourcing provider.

3.9 Email, internet and video monitoring

3.9.1 General rules

There are no specific rules for email and internet monitoring, except for employment relations (see section 3.6.2 below).

With respect to video monitoring, the Data Protection Commission has issued several guidelines, namely for monitoring in public spaces, employment relationships, shops and around private homes. In short, video monitoring is allowed in order to safeguard property, the safety of people or public order. A legitimate business interest may also be a ground for video monitoring, as long as this interest outweighs the privacy interests of the data subjects. As a basic principle, the public should be warned of video monitoring, for instance, with signs. Video monitoring should be implemented in a way that infringes privacy as little as possible. As a rule of thumb, video material may be kept only for 24 hours or as needed in order to solve a recorded incident.

Please note that under the Criminal Code the unlawful and secret recording of data communication may be a criminal act.

3.9.2 Employment relationship

In order to balance the interests of the data processor or data controller and the data subject, the Data Protection Commission has published a set of 'rules of thumb' for control of email and internet use by employees:

The general rules are the following:

- Treat online business the same way as offline business.
- Set clear rules with regard to the approval of the works council.
- Publish the rules in a manner accessible to the employee.
- Determine the extent to which private use of the facilities is permitted.
- Implement business software in such a way that the possibility of unauthorised use is disabled as much as possible.
- Create anonymous reports and usage statistics.

- Consider the backup of the system.
- Ensure the integrity of the system.
- Discuss observed behaviour as soon as possible.
- Provide access to the data.
- Evaluate the rules periodically.

The specific rules for email and internet are the following:

- Try to separate business and private email and try to avoid controlling private email.
- Limit targeted compliance checks to the previously stated goal.
- Limit general compliance checks.
- Limit logging traffic data. Store the log data for no longer than necessary.
- Do not include privileged information from works council members and occupational physicians in electronic messages.

Video monitoring may be implemented within a company when necessary to uphold a reasonable business interest, such as to protect property. Secret cameras may be used, as long as the employees and the works council have been informed up front that secret cameras may be used.

Pursuant to the Works Council Act, implementation of internal rules regarding monitoring email and internet or video surveillance are subject to prior approval from the works council.

4. INFORMATION OBLIGATIONS

4.10 Who

Data controllers are responsible for informing the data subjects about the processing of personal data relating to them.

4.11 What

The data controller should inform the data subject of its identity and the purposes of the processing for which the personal data are intended. Furthermore, the data controller should provide more detailed information on the circumstances in which the data are to be obtained or what use is to be made of them. This is necessary in order to guarantee that the processing is carried out in a proper and careful manner.

4.12 Exceptions

Information does not have to be provided where the data subject is already acquainted with the information. Furthermore, the Data Protection Act contains the following exceptions from the information obligation:

- if it appears to be impossible or would involve a disproportionate effort to provide the said information to the data subject. In that case, the data controller must however record the origin of the personal data; or
- if the recording or provision of the personal data is required by or under the law. In that case, the data controller must inform the data subject, upon his request, about the legal provision which led to the recording or supply of data relating to the data subject.

The requirement to provide information does also not apply where it is necessary in the interests of:

(a) state security;

(b) the prevention, detection and prosecution of criminal offences;
(c) important economic and financial interests of the state and other public bodies;
(d) supervising compliance with legal provisions established in the interests referred to under (b) and (c), or
(e) protecting the data subject or the rights and freedoms of other persons.

Also in connection with scientific research or statistics, or in the event of archiving regulated by law, the information obligation may be lifted.

4.13 When

Where the personal data are obtained from the data subject, he should be informed at the time the data are obtained. Where the data do not originate from the data subject, he must be informed at the time that the data relating to him are recorded or when it is intended to supply the data to a third party, at the latest on the first occasion that the said data are so supplied.

4.14 How

There are no specific rules on how the information should be provided, as long as the data subject has the information. Therefore, for instance, oral information can be sufficient under some circumstances.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

At the request of the data subject, the data controller has to inform him as to whether personal data relating to him are being processed. According to the Supreme Court an information request does not need to be substantiated. The Supreme Court has ruled that it may not suffice to provide a global overview of the data that are processed. Rather, the information a data controller is required to provide should be transparent and complete.

5.1.2 Exceptions

The data subject must take into account reasonable intervals when making requests. A data controller does not have to comply with an information request where this is necessary in the interests of:
(a) state security;
(b) the prevention, detection and prosecution of criminal offences;
(c) important economic and financial interests of the state and other public bodies;
(d) supervising compliance with legal provisions established in the interests referred to under (b) and (c); or
(e) protecting the data subject or the rights and freedoms of other persons.

Also in connection to scientific research or statistics the obligation to provide access may be lifted.

Courts have allowed exceptions in cases involving an incident register at a hospital; medical advice in a personal liability matter and a complaint commission within a company dealing with sexual harassment complaints. According to case law, the costs that have to be covered in order to comply

with information requests, are not recognised as a valid ground for an exception to the obligation to provide the information.

5.1.3 Deadline

The data controller has to inform the data subject in writing within four weeks as to whether personal data relating to him are being processed.

5.1.4 Charges

The data controller may require payment for expenses incurred in providing the information, which may not exceed EUR 5. The payment needs to be refunded in the event that the data controller corrects, supplements, deletes or blocks data at the request of the data subject, on the recommendation of the Data Protection Commission or by order of a court.

5.2 Rectification

5.2.1 Right

At the request of a data subject, the data controller should correct or supplement the personal data in the event that they are factually inaccurate, incomplete or irrelevant to the purpose or purposes of the processing, or are being processed in any other way which infringes a legal provision. This right may only be invoked where the data subject has used his right to access the data. Where personal data have been recorded on a data carrier to which no modifications can be made, the data controller must take the necessary steps to inform the data user that it is impossible to correct or supplement the data, even where there are grounds for modifying the data.

5.2.2 Exceptions

The right to rectify does not apply to public registers set up by law, where this law provides for a special procedure for correcting, supplementing, deleting or blocking data.

5.2.3 Deadline

The data controller shall inform the requester in writing within four weeks of receiving the request as to whether and, if so, to what extent, it is complying with it. A refusal to do so must be accompanied by the reasons for it. There is no deadline set in the Data Protection Act for the actual rectification but it should be executed as quickly as possible.

5.2.4 Charges

The data subject may not be charged for exercising his rectification right.

5.3 Erasure

5.3.1 Right

At the request of a data subject, the data controller should delete the personal data in the event that they are factually inaccurate, incomplete or irrelevant to the purpose or purposes of the processing, or are being processed in any other way which infringes a legal provision. This right may only be invoked where the data subject has used his right to access the data. Where personal

data have been recorded on a data carrier to which no modifications can be made, the data controller must take the necessary steps to inform the data user that it is impossible to delete the data, even where there are grounds for modifying the data.

5.3.2 Exceptions

The right to erase does not apply to public registers set up by law, where this law provides for a special procedure for correcting, supplementing, deleting or blocking data.

5.3.3 Deadline

The data controller shall inform the requester in writing within four weeks of receiving the request as to whether and, if so, to what extent, it is complying with it. A refusal to do so must be accompanied by the reasons for it. There is no deadline set in the Data Protection Act for the actual erasure but it should be executed as quickly as possible.

5.3.4 Charges

The data subject may not be charged for exercising his erasure right.

5.4 Blocking

5.4.1 Right

At the request of a data subject, the data controller should block the personal data in the event that they are factually inaccurate, incomplete or irrelevant to the purpose or purposes of the processing, or are being processed in any other way which infringes a legal provision. This right may only be invoked where the data subject has used his right to access the data. Where personal data have been recorded on a data carrier to which no modifications can be made, the data controller must take the necessary steps to inform the data user that it is impossible to block the data, even where there are grounds for modifying the data.

5.4.2 Exceptions

The right to block does not apply to public registers set up by law, where this law provides for a special procedure for correcting, supplementing, deleting or blocking data.

5.4.3 Deadline

The data controller shall inform the requester in writing within four weeks of receiving the request as to whether and, if so, to what extent, it is complying with it. A refusal to do so must be accompanied by the reasons. There is no deadline set in the Data Protection Act for the actual blocking, it should be executed as quickly as possible.

5.4.4 Charges

The data subject may not be charged for exercising his blocking right.

5.5 Objection

5.5.1 Right

In connection with his particular personal circumstances, a data subject has the right to object to the use of his personal data where they are used for processing that is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the data are provided or for processing that is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied.

In addition, a data subject has the right to object to the use of his personal data in connection to direct marketing (see section 3.3 above). The data subject does not have to substantiate such request.

5.5.2 Exceptions

The right to object based on particular personal circumstances does not apply to public registers set up by law.

5.5.3 Deadline

The data controller has four weeks to send a response. Where the objection is justified, the data controller must stop the processing with immediate effect.

Where the personal data are used for direct marketing, in the case of an objection, the processing must be stopped with immediate effect.

5.5.4 Charges

In the event of direct marketing, objection is free of cost. In other cases, the data controller may require a reasonable payment for expenses incurred.

5.6 Automated individual decisions

5.6.1 Right

A decision producing legal effects for a data subject, or materially affecting him, cannot be taken purely on the basis of automated data processing aimed at evaluating certain aspects of his personality.

5.6.2 Exceptions

The prohibition does not apply where the automated decision:

- has been taken in connection with the conclusion or execution of a contract, and: (i) the request of the data subject has been met; or (ii) appropriate measures have been taken to protect their legitimate interests; or
- is based on a law in which measures are laid down for protecting the legitimate interests of data subjects.

In the case of such an automated decision, the data subject has the right to be informed about the logic involved in any automated processing of data relating to him.

5.6.3 Deadline

The Data Protection Act contains no deadlines in connection to automated decisions.

5.6.4 Charges
Not applicable.

5.7 Other rights
Not applicable.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The notification obligations rest on the data controller.

6.1.2 What
Notification is required for all fully or partly automated processing of personal data intended to serve a single purpose or different related purposes.

6.1.3 Exceptions
Exceptions from the notification requirement are detailed in the Exemption Decree. A large number of socially well-known and accepted processing operations have been listed in it and are exempted from the notification obligation. They are subject to certain conditions, specified in the Decree. Such conditions, for instance, relate to the sorts of data, the retention period and the persons that have access to the data. If the conditions are not complied with, the processing is not exempted and should be notified.

The following registrations are, for instance, exempted under the Exemption Decree:

- administration of members or donors of associations or foundations;
- administration of subscriptions;
- staff administration;
- salary administration;
- accounts or equivalent administration of debtors and creditors;
- administration of customers and suppliers;
- administration of pupils and students or of former members, former staff members, former pupils or former students;
- personal data files that are kept for the internal administration of the holder's organisation; and
- personal data files containing data required for communication purposes.

6.1.4 When
Notification must be made prior to the processing of the data.

6.1.5 How
Notification must be made to:

- the Data Protection Commission; or
- if a data protection official has been appointed by the company, notification must be made to this official.

Notification can be made online or offline. To facilitate notification the Data Protection Commission has issued standard notification forms, both for offline as well as online use. The notifications forms are straightforward and

fairly easy to complete. They are available at: *www.cbpweb.nl/Pages/ind_melden.aspx*.

Notifications to the Data Protection Commission should be made in the Dutch language.

The notification must contain the following information:

- the name and address of the data controller;
- the purpose or purposes of the processing;
- a description of the categories of data subjects and of the personal data or categories of personal data relating to them;
- the recipients or categories of recipients to whom the personal data may be supplied;
- the planned transfers of personal data to countries outside the European Union;
- a general description allowing a preliminary assessment of the suitability of the planned measures to guarantee the security of the processing;
- the purpose or purposes for which the personal data or categories of personal data have been or are being collected.

The notification is valid from the moment that the contact person receives confirmation of receipt together with a number of the notification.

6.1.6 Notification fees

There is no notification fee.

6.2 Authorisation requirements

In principle, data controllers do not need to obtain authorisation to carry out a data processing activity. However, authorisation may be required for the transfer of personal data to a non-European Economic Area (EEA) country which does not provide an adequate level of protection (see section 8 below).

6.3 Other registration requirements

The Data Protection Act contains specific regulations for prior investigation, which come close to an authorisation requirement. Prior investigation is obligatory in the following situations:

- when numbers are used to identify individuals (for example, tax and social insurance numbers) for a purpose other than that for which those numbers are specifically intended, in order to link those data to personal data held by another data controller. This will apply except where permitted by law;
- when the data controller is planning to record personal data on the basis of its own observations, without informing the data subject of this fact (for example, hidden camera surveillance);
- when the data controller is planning to process criminal data or data on unlawful or objectionable conduct on behalf of third parties, but does not have the permit required under the Private Security Organisations and Detective Agencies Act (*Wet particuliere beveiligingsorganisaties en recherchebureaus*).

If prior investigation is required, this must explicitly be indicated when notifying the Data Protection Commission of the envisaged data

processing. Subsequently, the Data Protection Commission will conduct an initial investigation; this may take up to four weeks. The Data Protection Commission may subsequently inform the applicant that further investigation is necessary. This investigation may take up to 20 weeks. The data controller must postpone processing until the investigation has been completed, or until receiving notification that no further investigation will be conducted.

6.4 Register

The Data Protection Commission keeps a public register of notified data processing. This register may be consulted freely by anyone. The register is in Dutch and can be found at the website of the Data Protection Commission (*www.cbpweb.nl/asp/ORSearch.asp*). It contains the following information:

- Name and address of data controller.
- Type of processing (eg, salary processing).
- Purpose of the processing.
- Data subjects and categories of data.
- Recipients of the data.
- Whether there is transfer of personal data to countries outside the European Union.

7. DATA PROTECTION OFFICER

7.5 Function recognised by law

A data controller or organisation may appoint a data protection officer. This is not mandatory.

7.6 Tasks and powers

The data protection officer supervises the application of and compliance with the Data Protection Act. The statutory tasks and powers as laid down in the Data Protection Act give this officer an independent position in the organisation. The Data Protection Commission must be notified of all data protection officers and keeps a public register of them.

Data subjects may contact a data protection officer for information, inspection of their own processed personal data or for complaints.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Personal data may only be transferred to a country outside the European Union where such country guarantees an adequate level of protection. As a starting principle, the data controller is responsible for determining whether a certain country offers an adequate level of protection. An assessment of the adequacy of the level of protection should take account of the circumstances affecting a data transfer operation or a category of data transfer operations.

8.2 Legal basis for international data transfers

An international data transfer to a country that does not guarantee an adequate level of protection may take place, provided that:

- the data subjects have unambiguously given their consent;

- the transfer is necessary for the performance of a contract between the data subjects and the data controllers, or for actions to be carried out at the request of the data subjects and which are necessary for the conclusion of a contract;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between data controllers and third parties in the interests of data subjects;
- the transfer is necessary on account of an important public interest, or for the establishment, exercise or defence in law of any right;
- the transfer is necessary to protect a vital interest of the data subjects; or
- the transfer is carried out from a public register set up by law or from a register which can be consulted by anyone or by any persons who can invoke a legitimate interest, provided that in the case concerned, the legal requirements for consultation are met.

Alternatively, personal data may be transferred on the basis of an export permit. Such permits are issued by the Minister of Justice, after consulting the Data Protection Commission. The permit application form is available on the website of the Data Protection Commission, in Dutch (*www.cbpweb.nl/downloads_int/internationaal_aanvraagformulier_artikel_77.2_wbp_ne.pdf*) and English (*www.cbpweb.nl/downloads_int/internationaal_aanvraagformulier_artikel_77.2_wbp_en.pdf*). Applicants must submit the following information:

- Name of the data exporter.
- Name of the data importer.
- Data subjects.
- Purpose of the transfer.
- Categories of data (including whether sensitive personal data are transferred).
- Recipients.
- Retention period.
- Description of the type of transfer contract used (eg by indicating whether or not a model contract of the European Commission has been used, including amendments to it).
- Additional information (not obligatory).

A permit may be granted as quickly as five to six weeks after application. Best practice is to use one of the model contracts of the European Commission as a basis for the transfer, without any material amendments to it. Any material amendment may trigger the Data Protection Commission to require additional contracts or information and this may delay the process considerably.

Please note that a proposal to abolish this permit requirement if use is made of one of the European Commission's standard contractual clauses is currently being discussed in the Senate and is expected to enter into force the first half of 2012.

8.2.1 Data transfer agreements

A data transfer agreement as such is not sufficient to legitimise an international data transfer to an unsafe country. Therefore, in the case of a data transfer agreement, the transfer itself still needs to be based on one of

the grounds mentioned in section 8.2 above. Often parties have no option but to base the transfer on an export permit. This is even the case when one of the European Commission's standard contractual clauses for data transfers to third countries is used.

If the European Commission's standard contractual clauses are used, a permit will usually be provided within six to 12 weeks. Please note that any amendments to the standard contractual clauses will cause delays. Use of different contracts will also considerably delay the process.

8.2.2 Binding corporate rules

The Data Protection Commission is one of the forerunners with respect to binding corporate rules (BCRs). If a data transfer is based on BCRs, such data transfer must be authorised by the Minister of Justice, after consulting the Data Protection Commission. A permit application form can be found on the website of the Data Protection Commission. The process may take six weeks (when all relevant documents are provided).

The Netherlands participates in the so-called mutual recognition procedure. Therefore, if a lead authority in another country has accepted the BCRs, the Data Protection Commission will advise the Minister of Justice to authorise the transfer based on these BCRs.

8.2.3 Safe Harbour

There is no need for a specific legal ground (such as consent or an export permit) for international data transfers where the personal data are transferred to an organisation that is certified under the US Safe Harbour scheme and the data transfer falls into the scope of that certification. However, a processor agreement may still be required (see section 3.5 above).

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The Data Protection Act requires data controllers and data processors to ensure the confidentiality and security of personal data. In particular, confidentiality is regarded as an organisational security measure.

9.2 Security requirements

Data controllers and data processors should implement appropriate technical and organisational measures to secure personal data against loss or against any form of unlawful processing. These measures should guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures also aim to prevent unnecessary collection and further processing of personal data.

The Data Protection Commission has issued security guidelines in its report *Security of Personal Data* (*Beveiliging van persoonsgegevens*). These guidelines distinguish between four risk classes (0-III), depending on the impact that unlawful use of the data would have on the data subject. Per risk class the guidelines describe what organisational and technical security measures

should be implemented, such as having an information security policy and a secure access management system.

9.3 Data security breach notification obligation

Currently there is no obligation to notify individuals or the Data Protection Commission about the loss of personal data or data security breaches. At present, the non-profit organisation 'Bits Of Freedom' makes companies who breach security measures public on the internet. See also section 1.2 above.

9.4 Data protection impact assessments and audits

Data protection assessments and audits are recommended by the Data Protection Commission, but are not specifically mentioned in the Data Protection Act. It has developed a number of audit products in cooperation with auditors and third parties, such as a quickscan 'Data Protection Self-valuation and Privacy Audit Framework'. Using these audit products, organisations can verify the status of the protection of personal data in their organisation. These tools are available on the Data Protection Commission's website.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Data Protection Commission may adopt opinions and make recommendations, either of its own accord, or at the request of the government or third parties (in exceptional circumstances), on any matter relating to the application of the fundamental principles of the protection of privacy and personal data, not limited to the provisions of the Data Protection Act.

The Data Protection Commission may carry out targeted inspections on its own initiative. In addition, the Data Protection Commission may investigate complaints it receives. When the Data Protection Commission receives a complaint, it will, as a first stage, if it considers the complaint to be admissible, act as a mediator. If mediation between the parties fails, the Data Protection Commission can issue a non-binding opinion on the merits of the complaint. The opinion may contain recommendations for the data controller.

The Data Protection Commission may carry out on-site investigations. During the course of the investigation, the data controller must provide all necessary information upon request and co-operate with the Data Protection Commission. The Data Protection Commission is also entitled to exercise the right of access and rectification on behalf of a third party (indirect access).

In 2010 the Data Protection Commission performed 60 targeted audits and mediated in 172 complaints.

10.2 Sanctions

The Data Protection Commission has only a limited remit to impose fines. The Data Protection Commission can impose an administrative fine of up to EUR 4,500 for a violation of the notification obligation. In addition, the Data Protection Commission may, under the Police Data Act, also impose

an administrative penalty for breach of the protocol requirement as set out in that Act. In 2010 the Data Protection Commission did not impose any fines. There is currently a discussion as to how to expand the Data Protection Commission's power to impose fines, especially with regard to breaches of security and loss of personal data. As to violation of the Telecommunications Act (spam, cookies), the Telecom Authority (OPTA) may impose an administrative fine of up to EUR 450,000, or 10 per cent of the annual turnover of the company in violation.

The Data Protection Commission may also issue an administrative order on pain of a penalty sum if the provisions of the Data Protection Act are violated, ordering compliance with the Data Protection Act. In 2010 the Data Protection Commission gave 35 such orders.

Furthermore, data controllers who act in contravention of:

- the requirements to designate a person or body in the Netherlands to act on their behalf if they process personal data within the Netherlands without having an establishment; or
- the notification obligations; or
- a prohibition by the Minister of Justice to transfer data to a certain country,

may be prosecuted for a criminal offence. The penal fine for breaching the Data Protection Act is a maximum of EUR 3,700 (EUR 7,400 for companies). If the criminal offence was deliberate, the sanction is a penal fine up to EUR 7,400 (EUR 18,500 for companies) or a maximum of six years imprisonment.

10.3 Examples of recent enforcement of data protection rules

In 2008, 2009 and 2010 the Data Protection Commission did not impose any fines. In 2008 the Data Protection Commission issued 68 administrative orders, in 2009 26 orders and in 2010, 35 orders. With regard to breach of the spam regulation (Telecommunications Act), fines are more striking. A company sending SMS text messages was fined EUR 330,000 for sending paid messages to its targets.

10.4 Judicial remedies

A person suffering any harm as a consequence of acts infringing the provisions of the Data Protection Act can initiate a civil action for damages. We are not aware of any case law in which damages have been awarded.

10.5 Class actions

The Dutch Collective Settlements Act (*Wet collectieve afwikkeling massaschade*) provides for collective redress in mass damages. Mass damages may be redressed on the basis of a settlement agreement concluded between one or more representative organisations and one or more allegedly liable parties for the benefit of a group of affected persons to whom damage was allegedly caused. Once such a collective settlement is concluded, the parties may jointly request the Amsterdam Court of Appeal to declare it binding. If the Court grants the request, the agreement binds all persons covered by its terms and represented by the organisation, except for any person who has expressly elected to opt out within a specific period. Any person having opted out

retains his right to initiate individual proceedings against the defendant.

There have been no class actions with respect to data protection law infringements so far.

10.6 Liability

The data controller may be held liable for any damage as a result of an action in violation of the provisions of the Data Protection Act. Data subjects that have incurred damage from an action in violation of the Data Protection Act may thus claim damages from the data controller. The data controller shall be exempt from liability if he proves that the act which caused the damage cannot be ascribed to him. We are not aware of any case law in this respect.

Poland

Sołtysiński, Kawecki & Szlęzak Agata Szeliga

1. LEGISLATION

1.1 Name/title of the law

The basic rules on the processing of personal data are set forth in the Act on Personal Data Protection of 29 August 1997 (the PDP) which implements the EU Data Protection Directive 95/46/EC into the Polish legal system. More specific rules concerning processing of personal data may be found in other regulations, such as the Telecommunications Act, the Labour Code, Banking and Insurance Acts or in regulations concerning medical services or e-services. According to the PDP, if other acts establish a higher level of personal data protection than the level provided for in the PDP, these acts apply.

1.2 Pending legislation

As of 1 January 2012 the rules applicable to transfer of personal data to third countries ie, the countries not within the EEA, will change. At present, the transfer of personal data to a third party can take place only if the country of destination ensures the same level of protection in its territory as that in force in the territory of Poland. According to the new law, the personal data may be transferred to a third country if such third country ensures in its territory an adequate level of personal data protection. This 'adequate level of personal data protection' will be assessed taking into account all circumstances related to the data transfer operation, such as the categories of data, purpose and time of intended data processing operations, country of origin and country of final destination, laws of a given third country, as well as security measures and professional rules of conduct in force. Interestingly, the new law does not modify the provision of the PDP which states that that Data Protection Authority (GIODO) consent is required for the transfer of personal data to a third country if the third country does not ensure at least the same level of protection as Poland. Due to this inconsistency between PDP provisions, it is not clear whether the new law will achieve its goals. The strict reading of these provisions may lead GIODO to a conclusion that the regulations concerning transfer of personal data should not be applied as of 1 January 2012 differently from the way they are now.

In addition, also as of 1 January 2012, the rule which prohibits final resolution of the data subject's matter, if the content of such decision is based solely on automated processing of personal data in a computer system, will be softened. Namely, this rule will not apply either if the decision was issued during the conclusion or execution of an agreement and is in line with the application of the data subject, or if it is allowed by provisions

of law which should also provide for the measures protecting reasonable interests of data subjects. All these changes were adopted in connection with the new law concerning exchange of information, including personal data, between law enforcement agencies of the EU member states.

1.3 Scope of the law

1.3.1 The main players

The PDP applies both to public and private entities. The PDP defines a 'data controller' as a public authority, organisational unit, entity or person, who determines the purposes and means of personal data processing. Another category which is clearly defined in the PDP is the 'data recipient', ie, anyone to whom the personal data are disclosed, except for the data subject, a person authorised to carry out the data processing, a representative of the data controller from countries not being within the EEA, a data processor and state authorities or bodies of local government authorities to whom the data are disclosed in connection with ongoing proceedings.

The PDP does not ascribe precise meanings to terms such as 'third party', 'processor' or 'data subject'. These terms may be defined on the basis of other provisions in the PDP and jurisprudence. In particular, a 'processor' is viewed as an entity which processes personal data on behalf of the data controller, however, it does not have to be a separate legal entity. For example, a branch office may be a data processor for the headquarters, which is the data controller.

1.3.2 Types of data

Under the PDP the term 'personal data' means any information relating to an identified or identifiable natural person. An 'identifiable person' is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity; information is not regarded as identifying where the identification would require an unreasonable amount of time, cost and manpower. For example, a car's number plate does not constitute personal data because a significant amount of time, cost and manpower would be needed by a person other than a state authority to retrieve the personal data of the car's owner.

Special rules apply under the PDP to sensitive data (ie data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; religious; party or trade union membership; or data concerning health; genetic code; addictions or sex life; or data relating to convictions; decisions imposing penalties and fines; and other decisions issued in court or administrative proceedings).

The term 'personal data' does not include data on companies, authorities or other bodies. However, data belonging to self-employed individuals is subject to specific regulations. Namely, until 31 December 2011 the law states clearly that the PDP does not apply to the personal data of self-employed individuals which are entered into the official register of individuals conducting business activities. The Polish Data Protection

Authority issued an opinion that when this law expires the PDP will also not apply to such data, but different views have been expressed by some experts.

1.3.3 Types of acts/operations

The PDP determines the principles of personal data processing, ie, any operation which is performed upon personal data, such as collection, recording, storage, organisation, alteration, disclosure and erasure. The PDP applies both to processing in files, indexes, books or other registers, and to processing in IT systems, and also when the data are processed outside of a data filing system (the 'data system').

1.3.4 Exceptions

The PDP does not apply to:

- individuals who process data only for personal or household purposes;
- entities having their seat or place of residence outside of the EEA which use technical means located in Poland only for the transit of data.

Moreover, except for the provisions concerning security of processing and inspections, the PDP does not apply to press journalistic activity as defined in the Polish Press Act, and to literary and artistic activity, unless the freedom of expression and distribution of information significantly violates the rights and freedoms of the data subject. Similarly, only provisions on security of processing apply to data files prepared *ad hoc*, exclusively for technical or training purposes or in connection with education in high school, where the data are immediately deleted after being used or are anonymous.

1.3.5 Geographical scope of application

The PDP applies to individuals and legal persons, as well as organisational units not being legal persons, if they are involved in the processing of personal data as a part of their business or professional activity or in order to implement the statutory objectives, having their seat or place of residence in Poland or in a country outside of the EEA, if they are involved in the processing of personal data by means of technical devices located in Poland (which are not used for transit of data only). Thus, a limited liability company which has its core business operations in Poland, but which performs some operations on such data abroad is obliged to apply the PDP to such operations, irrespective of the application of that foreign law, which may impose some additional burdens.

1.3.6 Particularities

If the personal data are processed by the entities with their seat outside of the EEA, the data controller is obliged to nominate a representative in Poland.

2. DATA PROTECTION AUTHORITY

Generalny Inspektor Ochrony Danych Osobowych (GIODO)
General Inspector for Personal Data Protection

ul. Stawki 2
00-193 Warszawa
Poland
T: +48(22)8607086
F: +48(22)8607086
E: kancelaria@giodo.gov.pl
W: *www.giodo.gov.pl*

2.1 Role and tasks

The GIODO is the state authority responsible for protection of personal data.

The key tasks of the GIODO include:

- supervision to ensure the compliance of data processing with the PDP;
- issuing administrative decisions (in particular, approving the transfer of personal data to third countries or issuing post-inspection decisions) and reviewing complaints with respect to enforcement of the PDP;
- applying administrative enforcement measures in order to ensure the performance of non-monetary obligations arising from the decision referred to directly above;
- keeping a register of data systems and providing information regarding registered data files;
- issuing opinions on bills and regulations with respect to the protection of personal data;
- initiating and undertaking activities to improve the protection of personal data;
- participating in the work of international organisations and institutions involved in personal data protection.

2.2 Powers

The GIODO, including its authorised employees, have the right to access facilities, both private and public, where data systems or personal data are kept or processed and carry out inspections of such facilities or documents in order to assess compliance of the data processing with the PDP. This power cannot be exercised with respect to data systems which include classified information or data relating to members of churches or other religious unions with an established legal status, processed for the purposes of these churches or religious unions, or to data systems created as a result of inquiry procedures performed by officers of bodies authorised to conduct such inquiries by the Internal Security Agency, Intelligence Agency, Central Anticorruption Bureau and Military Information Services.

If the GIODO finds that the PDP has been violated, it may issue an administrative decision in which it orders the addressee to restore the proper legal status, in particular through completion, updating, correction, disclosure (or not), deletion of personal data or suspension of transfer of data to third countries. Moreover, if the GIODO comes to the conclusion that a given act or omission constituted a criminal offence described in the PDP, it has to report this offence to the competent authorities.

The GIODO also has the right to apply to other authorities or entities

with petitions aimed at ensuring more appropriate protection of personal data and the addressee of such a petition is required to respond within 30 days of receipt. The GIODO applies also to competent authorities with requests to commence the legislative process or issues opinions regarding bills concerning personal data protection.

2.3 Priorities

The key priority of the GIODO for the coming years, presented in the 2010 annual report, is the review of various Polish laws and regulations concerning personal data protection in order to ensure consistency, as well as introduction of modifications arising due to new technologies. The GIODO is particularly interested in social networking sites, cloud computing, internet browsers and their default settings, video-surveillance, localisation data and retention of telecommunications data. The GIODO would also like to increase the awareness of people with regard to their activities in the network and introduce 'the right to be forgotten' on the internet.

The second priority of the GIODO is providing its inspectors with a special certificate that authorises them to carry out inspections of special services (Police, the Internal Security Agency, etc). At present, in practice, no data processed by special services can be inspected by the GIODO. A court stated recently that the GIODO cannot assume in advance that all information collected about citizens by the special services is secret and cannot be reviewed by the GIODO. Thus, the GIODO should carry out checks to determine whether the special services comply with the PDP in areas in which the data are not secret. In addition, the GIODO would like to review secret data and in order to perform such operations, it will have to procure special certificates for its employees.

3. LEGAL BASIS FOR DATA PROCESSING

The PDP lays down the legal grounds based on which personal data may be processed. Special rules apply to sensitive data.

The PDP does not impose other conditions under which personal data may be transmitted/disclosed to a third party (other than to a data processor). The general rules concerning processing of data will apply to data transmission or disclosure.

3.1 Consent

3.1.1 Definition

A data subject's consent is the statement of will specifying consent to the processing of personal data by the person making the statement. This consent cannot be implied or derived from a different statement of will. Consent may be revoked at any time.

3.1.2 Form

Except for consent to processing of sensitive data and transfer to third countries which do not ensure an adequate level of personal data protection

– which should be given in writing – consent to other forms of data processing does not require any special form.

3.1.3 In an employment relationship

According to recent Polish court rulings, there are serious doubts as to whether consent may constitute a valid legal basis for data processing in an employment context. Such consent can be accepted only if it is given on a document separate from the employment contract and if it is possible to prove that the lack of such consent would not have an adverse effect on the employee in any respect.

3.2 Other legal grounds for data processing

Personal data may be processed without the consent of the data subject if:

- the processing is necessary to exercise rights and duties resulting from a legal provision;
- the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- the processing is necessary for the performance of tasks provided for by law and carried out in the public interest; or
- the processing is necessary for the purpose of the legitimate interests pursued by the data controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject. According to the PDP, the 'legitimate interests' of the data controllers are in particular direct marketing of own products or services provided by the controller or enforcement of claims related to conducted business activity.

It is worth noting that certain specific rules apply to the processing of employees' data. Pursuant to the Polish Labour Code, an employer may request that its employees provide the following data only:

(i) first and last names;
(ii) parents' first names;
(iii) date of birth;
(iv) address;
(v) education;
(vi) career path;
(vii) other personal data, including the names and dates of birth of children, to the extent they are necessary for the employee to enjoy the various rights granted to him/her under labour law;
(viii) identification number awarded by the authorities (so-called 'PESEL' number); and
(ix) other personal data, if the obligation to provide them stems from separate provisions of law.

The GIODO has expressed the opinion, upheld by some court rulings, that an employer cannot request from an employee data other than those listed above, even if the employee expressly agrees to provide such additional data. The aims of data processing are not defined in the Polish

Labour Code and in this respect, the general principles of the PDP apply, taking into account the limitations outlined above.

It is prohibited to process sensitive data except when one of the following situations occurs:

- the data subject has given his/her written consent, unless the processing consists of deletion of personal data;
- specific provisions found within other laws provide for the processing of such data without the data subject's consent and provide for full safeguards;
- the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent until a guardian or a probation officer is appointed;
- the processing is necessary for the purpose of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non-profit-seeking organisations or institutions with a political, scientific, religious, philosophical, or trade-union aim and provided that the processing relates solely to the members of those organisations or institutions or to persons who have regular contact with them in connection with their activity and subject to providing appropriate safeguards of the processed data;
- the processing relates to the data necessary to pursue a legal claim;
- the processing is necessary for the purposes of carrying out the obligations of a data controller with regard to employment of his/her employees and other persons, and the scope of processing is provided for by the law;
- the processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a healthcare professional, involved in treatment, other healthcare services, or the management of healthcare services and full safeguards are in place;
- the processing relates to data made public by the data subject;
- it is necessary to conduct scientific research including preparations of a thesis required for graduating from university or receiving a degree - any results of scientific research shall not be published in a way which allows data subjects to be identified;
- the processing is conducted by a party to exercise rights and duties resulting from decisions issued in court or administrative proceedings.

3.3 Direct marketing and cookies

The direct marketing of own goods and services of a data controller is regarded as a legally justified purpose for data processing. Thus, data controllers do not need to procure the consent of data subjects to process their data for that purpose. However, in order to safeguard the interests of data subjects, the PDP grants the data subject two basic rights. First, the data subject may submit, giving reasons, a written request that processing of his/her data for marketing purposes is ceased due to his/her special situation. If the data controller receives such a request it either ceases processing the

data or forwards the request to the GIODO, which issues a decision on the matter. Second, the data subject may raise objections if the data controller intends to process his/her data for direct marketing purposes. If such an objection is filed, the data controller cannot continue to process the data. He may only retain the first and last name, address and PESEL number to avoid a situation in which the data of that person is used again for marketing purposes (the so-called 'Robinson' list).

The Polish Electronic Services Act also specifies that it is prohibited to send unsolicited commercial communication via email or other electronic means of communication to an identified addressee without his/her consent. Entities which provide services through electronic means may store IT data, including cookies, in terminal equipment of the subscriber or end user which are designated for using such services provided that:

- the subscriber or end user is provided with clear and comprehensive information about the purpose of storing such data and the ways in which it will be used;
- the subscriber or end user is provided with clear and comprehensive information as to how to raise objections, which will in future make it impossible to store that data of the service provider in that terminal equipment; and
- the stored data do not cause changes in the configuration of terminal equipment or in the software installed on the equipment.

The above rules do not apply if the storage or access to the data stored is necessary to perform or facilitate transmission through a public network or if storage is necessary to deliver services provided via electronic means, and this has been requested by the end user or the subscriber.

Entities which provide services through electronic means may also install the software on terminal equipment of the end user or the subscriber or use such software. However, before starting such operations, the service provider should provide the end user or the subscriber with clear and comprehensive information regarding the purposes for installation of such software and the ways it will be used, as well as with information as to how to delete the software from the terminal and the end user or subscriber should agree to installation and use of such software by the service provider.

It should be stressed that as at 5 September 2011, Poland had not implemented Directive 2009/136/EC amending the e-Privacy Directive 2002/58/EC. The drafts of the implementing laws have not yet been presented to parliament.

3.4 Data quality requirements

The data controller should protect the interests of data subjects with due care, and in particular ensure that:

- the personal data are processed lawfully;
- the personal data are collected for specified and legitimate purposes and not processed further in a way incompatible with the intended purposes, unless this is allowed under the PDP;
- the personal data are relevant and adequate for the purposes for which

they are processed;
- the personal data are kept in a form which permits identification of the data subjects no longer than it is necessary for the purposes for which they are processed.

The processing of data for purposes other than intended at the time of data collection is allowed provided that it does not violate the rights and freedoms of the data subject and is done for the purposes of scientific, didactic, historical or statistical research or is allowed under the legitimate purposes of data processing specified in the PDP, and fulfilment of a disclosure obligation.

3.5 Outsourcing

According to the PDP, a data controller may contract the processing of personal data to another entity or person. This requires a contract between the data controller and the data processor, which should be concluded in writing. The contract should specify the scope and the purpose of data processing. Moreover, the PDP requires the data processor to implement security measures, and with respect to compliance with this obligation, the data processor is liable in the same way as the data controller. The data controller is liable towards data subjects or other third parties for the compliance of the data processor with the PDP. The GIODO is explicitly authorised to carry out inspections of data processors.

3.6 Email, the internet and video monitoring

3.6.1 General rules

There is no one law in Poland that regulates all aspects of email, internet and video monitoring. Specific issues concerning monitoring may be found in some legal acts, such as sports legislation law, legislation on mass events, or in various criminal laws.

Therefore, in civil law relationships, the rules concerning email, internet and video monitoring are derived from the concept of protection of so-called 'personal interests' of data subjects expressed in the Civil Code, which includes the right to protect privacy, as well as from the PDP and the Telecommunications Act.

Due to the lack of detailed legal regulations concerning email, internet and video monitoring, the GIODO usually follows the recommendations expressed in the opinions of the Data Protection Working Party, which was set up under Article 29 of Directive 95/46/EC.

Based on the above, as well as on limited jurisprudence, the following basic rules apply. First, in order to make the monitoring legitimate, the data subjects should be aware that the monitoring will be performed. Naturally, the disclosure obligation does not apply in particular when the law states that the monitored person does not have to be informed (usually in criminal investigations), if the data subject has agreed to such monitoring or if it is clear that the monitored person is abusing its personal interests (for instance, if he uses his private emails to receive or send illegal content). However, all exceptions should be interpreted narrowly.

Second, the general rules for legitimate processing of personal data, such as legitimacy, proportionality, and transparency should be observed.

It should be also noted that in court proceedings evidence collected through monitoring which does not fulfil these requirements may be rejected by the court.

3.6.2 Employment relationship

There are no specific rules concerning monitoring of employees in Poland. However, there are more GIODO guidelines and more jurisprudence in this area compared to monitoring in general.

It follows from the above that such monitoring will be found acceptable if:

- it is justified under the law;
- it is proportionate and adequate to the purpose which is to be achieved (for example, it is not possible to achieve legitimate goals of the employer in other ways);
- the employee should be informed about monitoring, as well as what kind of data will be collected and for what purposes they will be used. This requirement is not strict and it is accepted that the employees may not be informed before the monitoring starts if significant interests of the employer are at stake (for example, it is possible to use video monitoring of the employees without notice if based on other circumstances, it is very likely that these particular employees are responsible for thefts of employer property).

It should be added that the consent of the employee to such monitoring would not legitimise such operations because, taking into account the nature of the employment relationship, it is difficult to argue that the lack of consent would not affect the employee's situation. Thus, the consent to monitoring is not given freely.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers have the obligations specified below.

4.2 What

The data controller should provide the data subjects with its name and address, the purpose of the data processing, data recipients or their categories, the right to access the data and to rectify it, as well as whether the data are collected voluntarily or under an obligation arising from the law (in the latter case, the legal basis should be provided). When data controllers collect the data from persons other than the data subject, they do not have to provide them with the information but instead are required to indicate the source of the data and inform the data subject about the right to raise an objection or request (with reasons) that the data processing for the performance of tasks provided for by law and carried out in the public interest or for the purpose of the legitimate interests pursued by the data controllers or data recipients, be ceased.

4.3 Exceptions

When the data controller collects personal data directly from the data subject, it does not have to notify him/her if other legislation allows for personal data processing without disclosure of the real purpose for which the data are collected or if the data subject already has the required information.

When the personal data are not collected from the data subject, in addition to the exceptions listed above, the notification is not necessary if the data are necessary for scientific, didactic, historical, statistic or public opinion research and the processing of such data does not violate the rights or freedoms of the data subject while the fulfilment of the notification obligation would involve disproportionate efforts or endanger the success of the research, or if the data are processed by the state or local authorities, their organisational units or by non-public entities performing public duties on the basis of the law.

4.4 When

The PDP states that the data controller has the obligation to inform the data subject promptly after recording the personal data collected from a third party. There is no such clear obligation expressed in law which imposes disclosure obligations on data controllers collecting data directly from the data subject, but according to legal doctrine, this should be done without delay.

4.5 How

There are no special requirements. For evidence purposes, written form or email is often used.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The obligation to ensure the right to access the personal data is vested with the data controllers. The right to access the data has been granted to the persons to whom the data relate (data subjects). If the data relates to a data subject who is underage or does not have full legal capacity, the general rules of representation apply. In particular, a request may be submitted by a child's parent.

5.1.2 Exceptions

The information does not have to be provided if it would cause:

- disclosure of information which includes classified information (ie, information the unauthorised disclosure of which would cause or could have caused damage to Poland or which would have an adverse effect on its interests and includes information in the preparation phase, irrespective of form and way of expression);
- a threat to state defence or security, life or health of people or public safety and order;
- a threat to basic economic or financial state interest; or
- a significant infringement of the personal interest of data subjects or

other persons.

Moreover, if the data are processed for scientific, educational, historical, statistic or archival purposes, the data controller may decide not to inform the data subjects that their data are being processed if this would lead to expenses disproportionate to the intended effect.

5.1.3 Deadline

The data subject may request information once every six months. The information should be provided within 30 days.

5.1.4 Charges

The PDP does not give the data controller the right to charge the data subject for exercising its rights. The courts confirmed that such charges cannot be collected.

5.2 Rectification

5.2.1 Right

The person to whom the personal data relate may demand that the data are completed, updated or rectified in cases in which they are incomplete, outdated, untrue or collected in violation of the PDP, or if they are no longer required for the purpose for which they were collected.

5.2.2 Exceptions

None.

5.2.3 Deadline

None.

5.2.4 Charges

Please refer to section 5.1.4.

5.3 Erasure

5.3.1 Right

The person to whom the personal data relate may demand that the data be deleted if they are incomplete, outdated, untrue or collected in violation of the PDP, or if they are no longer required for the purpose for which they were collected.

5.3.2 Exceptions

None.

5.3.3 Deadline

None.

5.3.4 Charges

Please refer to section 5.1.4.

5.4 Blocking

5.4.1 Right

The person to whom the personal data relate may demand that the data controller temporarily or permanently cease processing the data if they are incomplete, outdated, untrue or collected in violation of the PDP, or if they are no longer required for the purpose for which they were collected.

5.4.2 Exceptions

None.

5.4.3 Deadline

None.

5.4.4 Charges

Please refer to section 5.1.4.

5.5 Objection

5.5.1 Right

The person to whom the data relate may object to the processing of his/her personal data or submit a demand with reasons that processing of his/her data be ceased due to his/her particular situation if the personal data are processed for the performance of tasks provided for by law and carried out in the public interest or for the purpose of the legitimate interests pursued by the data controllers or data recipients.

5.5.2 Exceptions

If an objection is raised, the data controller may still process the first and last names, as well as identification number and the address of the data subject only in order to prevent use of that person's data again for the purposes covered by the objection.

5.5.3 Deadline

The data controller should immediately cease processing the personal data, or in the case of a justified request, forward the case to the GIODO for issuance of a decision.

5.5.4 Charges

None.

5.6 Automated individual decisions

5.6.1 Right

The person to whom the data relate may request that the data controller reconsiders the individual case settled in contravention of the rules applicable to issuance of the decisions the content of which is solely the result of operations on data in the IT system.

5.6.2 Exceptions

None.

5.6.3 Deadline
The data controller should either review the case without delay or forward it to the GIODO to be resolved.

5.6.4 Charges
None.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
The notification obligations rest with the data controller or a representative of the data controller.

6.1.2 What
The data controller should submit the data system for registration by the GIODO.

6.1.3 Exceptions
Data controllers do not have to submit information about data systems which contain data:
- constituting classified information;
- collected as a result of inquiry procedures performed by officers of the bodies authorised to conduct such inquiries;
- processed by relevant bodies for the purpose of court proceedings and on the basis of National Criminal Register legislation;
- processed by the Inspector General of Financial Information;
- processed by relevant bodies for the purpose of the participation of Poland in the Schengen Information System and the Visa Information System;
- relating to the members of churches or other religious unions with an established legal status, being processed for the purposes of those churches or religious unions;
- processed in connection with the employment by the data controller or the providing of services for the data controller on the grounds of civil law contracts, and also which refers to the data controller's members and trainees;
- referring to persons availing themselves of their healthcare services, notarial or legal advice, patent agents, tax consultants or auditor services;
- created on the basis of election regulations concerning the Polish Parliament, European Parliament, local councils, the President of the Republic of Poland, head of the commune, elections of a town or city mayor, and the acts on a referendum and municipal referendum;
- referring to persons deprived of freedom under the relevant law within the scope required for carrying out the provisional detention or deprivation of freedom;

- processed for the purpose of issuing an invoice, a bill or for accounting purposes;
- that are publicly available;
- processed to prepare a thesis required to graduate from a university or be granted a degree; or
- processed with regard to minor current everyday affairs.

6.1.4 When

The decision of the GIODO regarding registration of a data system containing sensitive data should be issued before the data controller starts processing that data in the data system. With respect to non-sensitive data, the notification should be made prior to the start of data processing, unless the data controller is released from the notification obligation.

The data controller should notify the GIODO of any changes in information submitted to the GIODO within 30 days from making the change in the data system, provided that if the data controller extends the scope of processed data to include sensitive data, the data controller should notify the GIODO of that change before it is actually made.

6.1.5 How

The notification should be made in the Polish language on the standard form which is currently provided for in the Decree issued by the Minister for Internal Affairs and Administration of 12 December 2008. The notification is submitted to the GIODO either as a hard copy, or online via the website *www.egiodo.gov.pl* or by email. If the notification is submitted via the website or email, it should be signed with a secure electronic signature. In the absence of an electronic signature, the applicant should submit a hard copy in addition to the electronic application.

The notification for registration of the data system should include:

- an application to enter the personal data system into the register;
- name and address of the data controller, including the identification number in the register of enterprises (REGON), and the legal grounds on which it is authorised to run the data system, and in the case of outsourcing of data processing or appointment of a representative, the name and the address of the data processor or representative;
- the purpose of the data processing;
- description of the categories of data subjects and the scope of the processed data;
- information on the ways and means of data collection and disclosure;
- information on the recipients or categories of recipients to whom the data may be transferred;
- a description of the technical and organisational measures employed for the purposes of the protection of personal data;
- information regarding the ways and means of fulfilling such technical and organisational conditions; and
- information relating to possible data transfer to a third country.

If the application is signed by an attorney, the power of attorney should be attached to the notification.

The GIODO has received around 8,000 notifications per year over the past three years. According to information on the GIODO website, in 2010, the GIODO received 8,459 notifications and registered 5,644 data systems. The length of the notification process differs and may last from one month to several months.

6.1.6 Notification fees

There are no notification fees.

6.2 Authorisation requirements

6.2.1 Who

The obligation to obtain authorisation (consent) rests with the data controllers.

6.2.2 What

At present, the consent of the GIODO is required for the transfer of personal data to a third country, ie a country which does not belong to the EEA, if that country does not ensure at least the same level of personal data protection as that in force within the territory of Poland and the statutory premises for lawful transfer of personal data are not met.

6.2.3 Exceptions

If the premises for lawful transfer of personal data to third countries, as indicated in the PDP, are met, the consent of the GIODO for such transfer is not required.

6.2.4 When

The consent of the GIODO for transfer of data to third countries should be procured before the transfer takes place. It is not necessary to renew such consent.

6.2.5 How

The application should be made in Polish. There is no standard form for this application. The application is submitted to the GIODO as a hard copy, or online via the website *www.giodo.gov.pl/432/id_art/2096/*or via email. If the notification is submitted via the website or email, it should be signed with a secure electronic signature. In the absence of an electronic signature, the applicant should submit a hard copy in addition to the electronic application.

The application should specify, in particular:

- the name and address of the applicant;
- the application for a decision allowing transfer of personal data;
- the name and address of the data recipients and whether they are the data controllers or data processors;
- the categories of data subject and scope of personal data transferred to

third countries;
- a description of technical and organisational measures applied for the purposes of protection of the personal data; and
- information regarding the ways and means of fulfilling such technical and organisational conditions.

If the application is signed by an attorney, the power of attorney should be attached to the notification.

In 2010, the GIODO received 37 applications for authorisation of data transfer to third countries. The length of the authorisation proceedings differs. On average it lasts between three to several months.

6.2.6 Authorisation fees

There is a fee in the amount of 10 PLN (approximately €2.5) for issuance of the decision.

6.2.7 Other registration requirements

In Poland, prior checks are carried out with respect to sensitive personal data. Namely, as mentioned above, data controllers may start to process such data after the GIODO registers the data system.

6.3 Register

Except for the register of data systems, there are no other registers related to personal data processing. The register, which is open to the public, is available at: *www.egiodo.gov.pl* and contains the following information:
- name of the data system;
- name and address of the data controller, including the identification number in the register of enterprises (REGON), and the legal grounds on which it is authorised to run the data system, and in the case of outsourcing of data processing or appointment of a representative, the name and the address of the data processor or representative;
- the purpose of the data processing;
- description of the categories of data subjects and the scope of the processed data;
- information on the ways and means of data collection and disclosure;
- information on the recipients or categories of recipients to whom the data may be transferred;
- information relating to possible data transfer to a third country.

Information about decisions regarding transfer of personal data to third countries issued in a given year may be found in the annual GIODO report.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The data controller should appoint a data protection officer (DPO). However, when the data controller is natural person, it may decide to perform the duties of the DPO personally.

7.2 Tasks and powers

The key responsibility of the DPO is to supervise the compliance of a data controller with rules for protection of personal data. Therefore, the DPO is usually responsible for implementation and updates of internal documents required by PDP secondary legislation, such as security policy and IT management instruction, as well as for maintenance of a register of persons authorised to process personal data.

The appointment of the DPO does not release the data controllers from any obligations.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The transfer of personal data within the EEA is allowed on the basis of the PDP. However, the transfer of personal data to a third country, ie the country which does not belong to the EEA, is allowed if that third country ensures at least the same level of protection as the one in force in Poland. As mentioned above, the above rule will change as of 1 January 2012. As of that date the personal data may be transferred to a third country if such third country ensures in its territory an adequate level of personal data protection. This 'adequate level of personal data protection' will be assessed taking into account all circumstances related to the data transfer operation, such as the categories of data, purpose and time of intended data processing operations, country of origin and country of final destination, laws of a given third country, as well as security measures and professional rules of conduct in force.

8.2 Legal basis for international data transfers

If a given third country does not ensure the level of personal data protection required by PDP, the data controller may still transfer the personal data to that country, provided that:

- the transfer of personal data is required by legal provisions or by any ratified international agreement;
- the data subject has given his/her written consent;
- the transfer is necessary for the performance of a contract between the data subject and the data controller or takes place in response to the data subject's request;
- the transfer is necessary for the performance of a contract concluded for the benefit of the data subject between the data controller and another subject;
- the transfer is necessary or required due to the public interest or for the establishment of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer relates to data which are publicly available.

If none of the above conditions are met, the data may be transferred to third countries which do not ensure at least the same level of personal data protection as Poland once the GIODO grants its consent provided that the data controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject. The new law which

enters into force on 1 January 2012 thus removes the requirement that the adequate level of protection of personal data in the third country is assessed taking into account the standard of personal data protection in Poland. However, this new law does not modify this provision of the PDP which states that that GIODO consent is required if the third country does not ensure at least the same level of protection as Poland and the conditions outlined in the bullets above are not met. Due to this inconsistency, it is not clear whether the new law will achieve its goals. The strict reading of these provisions may lead GIODO to a conclusion that the regulations concerning transfer of personal data should not be applied as of 1 January 2012 differently from the way they are now.

8.2.1 Data transfer agreements

The PDP does not set any special requirements for data transfer agreements. At present, the consent of the GIODO for the transfer of personal data to the third country is required even if the data importer and data exporter have entered into the standard contractual clauses adopted by the European Commission. However, execution of such clauses usually simplifies the proceedings before the GIODO as it is perceived as a measure which ensures adequate safeguards for the personal data. Therefore, most of the data exporters decide to use the standard contractual clauses adopted by the European Commission. After 1 January 2012 and entry of the new law into force, one may argue that if the data importer and data exporter enter into the standard contractual clauses adopted by the European Commission the consent of GIODO is no longer required. However, due to the abovementioned inconsistency between the PDP provisions, until GIODO works out its position, the prudent approach is to apply for GIODO consent.

8.2.2 Binding corporate rules

The PDP does not set any special requirements for binding corporate rules. The GIODO has stated that the entities interested in this instrument should follow the guidelines issued by the Data Protection Working Party. The consent of the GIODO for the transfer of personal data to a third country is required at present even if the data importer and data exporter have implemented such rules. However, the adoption of such rules usually simplifies the proceedings before the GIODO as it is perceived as a measure which ensures adequate safeguards for data.

The procedure to obtain GIODO consent is the same as for transfers of personal data to third countries. Thus, an applicant should file with GIODO an application for approval of binding corporate rules. The application should be made in Polish. There is no standard form for this application. The application is submitted to the GIODO as a hard copy, or online via the website *www.giodo.gov.pl/432/id_art/2096/*or via email. If the notification is submitted via the website or email, it should be signed with a secure electronic signature. In the absence of an electronic signature, the applicant should submit a hard copy in addition to the electronic application.

The application should specify, in particular:

- the name and address of the applicant;
- the application for a decision allowing transfer of personal data;
- the name and address of the data recipients and whether they are the data controllers or data processors;
- the categories of data subject and scope of personal data transferred to third countries;
- a description of technical and organisational measures applied for the purposes of protection of the personal data, including copy of the binding corporate rules and information whether they have been approved by any EU member state; and
- information regarding the ways and means of fulfilling such technical and organisational conditions.

If the application is signed by an attorney, the power of attorney should be attached to the notification.

As mentioned above, the interpretation that GIODO consent is required may change as of 1 January 2012, when the amendments to the PDP enter into force.

So far, the binding corporate rules have not been popular in Poland and most companies decide to use the standard contractual clauses. Poland is also not a part of the mutual recognition procedures for binding corporate rules.

8.2.3 Safe Harbour

The GIODO confirmed previously that the transfer of personal data to a recipient with its seat in the US, participating in a safe harbour scheme, is regarded as the transfer of such data to a third country which offers an adequate level of protection.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Persons authorised to carry out the processing of personal data are obliged to keep this personal data and the ways in which they are protected confidential. That obligation is not limited in time.

9.2 Security requirements

The data controllers and the data processors have to implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and in particular they are obligated to protect personal data against unauthorised disclosure, takeover by an unauthorised person, processing in violation of the PDP, and any change, loss, damage or destruction.

Detailed security requirements are specified in the Decree issued by the Minister for Internal Affairs and Administration of 29 April 2004. The PDP itself neither defines the 'technical' nor the 'organisational' measures, nor specifies which measures should qualify as technical and organisational measures.

The PDP obliges the controller and processor to keep documentation describing the way in which data are processed and measures implemented

to safeguard personal data. The security policy and IT system management instruction constitutes this documentation, and should be constantly updated.

The security policy should contain, in particular, a list of buildings or premises where personal data are processed, the list of data systems and the software used for processing, a description of the structure of data systems, flow of data between various systems, or measures which are implemented in order to ensure confidentiality, integrity and accountability of processed data.

The IT system management instruction specifies in particular the procedures for granting authorisation for data processing and recording that information in IT systems, as well as the person responsible for these tasks, authorisation methods, backup copy procedures, and where and how long the media with personal data and backup copies are stored.

Detailed guidelines concerning the content of these documents have been adopted by the GIODO and are available on its website.

Polish law establishes three security levels for processing of personal data in an IT system:

- basic, which should be applied when only non-sensitive data are processed and none of the IT system devices are connected to a public telecommunications network;
- increased, which should be applied if the sensitive data are processed and none of the IT system devices are connected to a public telecommunications network;
- high, which should be applied if at least one device of an IT system used to process data is connected to a public telecommunications network.

For all security levels, the following measures described briefly below should be applied.

9.2.1 IT systems, hardware and media

For each person whose personal data are being processed within the IT system, except for the systems used for personal data processing, that system should secure keeping records of:

- the date when the data have been registered for the first time in the system;
- an identifier of a user who registers the personal data in the system, unless the access to the computer system and personal data being processed within this system is available to one person only;
- data sources, in cases where the data have not been obtained from the data subject;
- information on data recipients to whom the data have been disclosed and the date and the scope of this disclosure, unless the IT system is used for the processing of personal data contained in open data systems;
- any objection raised by the data subject, when the personal data are to be processed for marketing purposes or there is an intent to transfer them to other data controllers.

The access control mechanisms should be applied in the IT system used for personal data processing. If the access to personal data is granted to at

least two persons it should be ensured that a separate identifier is registered for each user of the IT system and access to data is granted only after entering the identifier and user's authentication.

The IT system used for personal data processing should be secured, in particular, against computer viruses or other software used for gaining unauthorised access to the IT system and loss of data which may be caused by any power supply failure or line interference.

Where a password is used for user authentication, it should be changed at least once a month. The password has to consist of at least six characters (for increased and high security levels – eight characters passwords are required). When the high security level applies, the data controller should apply cryptographic protection measures for the data used for authentication which are being transferred within the public network.

The personal data processed within the IT system should be secured through back up copies of the data systems and use of data processing software. Back up copies should be stored in the premises ensuring security against any unauthorised takeover, change, damage or destruction, as well as be deleted as soon as they are no longer useful.

Media and hardware on which personal data are stored should be handled in the way which protects the personal data against unauthorised disclosure. In particular, all personal data should be deleted from phones, computers or other electronic devices which are to be liquidated or transferred to third parties.

9.2.2 Physical protection

The area when the personal data are processed should be secured against access from unauthorised persons during the absence in this area of the persons authorised to process personal data. Any unauthorised person may stay inside that area only with the data controller's consent or in the presence of a person authorised to process personal data.

9.3 Data security breach notification obligation

Under the PDP there is no obligation to notify individuals or the GIODO of any data security breaches. It is worth mentioning that a person who, being a controller of a data system, violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised takeover, damage or destruction, shall be subject to criminal liability (a fine, the penalty of restriction of liberty or imprisonment up to one year). As the GIODO is under a statutory obligation to report such an offence, even voluntary notification of the GIODO may lead to criminal sanctions. In 2010, the GIODO reported one offence consisting of disclosure of personal data to the unauthorised person.

9.4 Data protection impact assessments and audits

There is no legal requirement to carry out data protection impact assessments and audits and the GIODO does not provide detailed guidelines in this respect.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The GIODO may issue a decision obliging the addressee to comply with the PDP. In particular, the GIODO may demand that the personal data be completed, updated, corrected, disclosed or not disclosed to a third party. The GIODO may also suspend the transfer of the data to third countries or order that the data are deleted. The decisions may be issued upon the request of an interested party or *ex officio*. In 2010, the GIODO issued 137 decisions in relation to the inspections carried out by the GIODO and 359 decisions were issued as a result of complaints of interested parties.

As mentioned above, the GIODO also has the obligation to report offences related to processing of personal data to competent law enforcement authorities. In 2010, the GIODO reported 23 offences, 18 of which were based on the complaints of individual data subjects. The remaining five reports were the outcome of inspections carried out by the GIODO. The statistics presented by the GIODO show that most of these notifications are not pursued by the law enforcement authorities.

10.2 Sanctions

The PDP provides for the following criminal sanctions:

- a person who processes the personal data in the data system when such processing is not allowed or he is not authorised to perform such processing, shall be subject to a fine, penalty of restriction of liberty or imprisonment up to two years, provided that if such act is performed with respect to sensitive data, the maximum penalty of imprisonment is three years;
- a person who, being a data controller or being obliged to protect personal data, discloses or enables the access to such data to unauthorised persons shall be subject to a fine, the penalty of restriction of liberty or imprisonment for up to two years. If such person was not acting intentionally, the maximum penalty of imprisonment is one year;
- a person who, being a data controller of a data system, violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised takeover, damage or destruction, shall be subject to a fine, the penalty of restriction of liberty or imprisonment for up to one year;
- a person who, being obliged, does not apply for the registration of the data system shall be subject to a fine, the penalty of restriction of liberty or imprisonment for up to one year;
- a person, who being a data controller, does not notify the data subject about its rights or does not provide the data subject with information allowing him/her to make use of its rights granted by the PDP shall be subject to a fine, the penalty of restriction of liberty or imprisonment for up to one year;
- a person who makes it impossible for the inspector to perform the inspection activities or obstructs performance of such activities shall be subject to a fine, the penalty of restriction of liberty or imprisonment for

up to two years.

The GIODO does not have currently the right to impose financial penalties for breach of the PDP.

10.3 Examples of recent enforcement of data protection rules

The PDP is enforced in practice. The GIODO acts through its decisions, which are subject to judicial control. In 2010, the administrative courts issued 95 rulings in relation to decisions issued by the GIODO. In particular, in August 2010, the administrative court of first instance upheld the decision of GIODO obliging a company to notify the data subjects whose personal data were retrieved from the official, publicly available court registers and stored in the data system created by the company. The administrative court agreed with GIODO that the consent of data subjects to disclose their data in the publicly available court register does not imply their consent to commercial processing of their data by third parties. In another ruling, issued in December 2009, the Supreme Administrative Court upheld the decision of GIODO prohibiting the company from processing the fingerprints of employees for the purpose of recording their work time. This ruling was important due to the fact that the court clearly expressed the view that the consent of the employee to the processing of his/her personal data does not usually legitimise the processing of these data, as such consent is not given voluntarily due to the unbalanced relationship between the employer and employee.

The GIODO also reports offences related to data processing to competent law enforcement authorities. As mentioned above, most of these notifications are not pursued by the law enforcement authorities. For example, in 2010 only one case was filed with the court and the convicting sentence was also issued only in one case.

In addition, the data subjects may pursue their rights individually based on civil law liability.

10.4 Judicial remedies

The addressee of the decision issued by the GIODO has the right to apply to the GIODO for re-examination of the case. The decision issued by GIODO after such re-examination may be challenged by the party to the administrative court of first instance. From the ruling of that court, both GIODO and the other party may appeal to the Supreme Administrative Court. As mentioned above, in 2010, there were 95 rulings issued by the administrative courts of both instances concerning the decisions of the GIODO.

10.5 Class actions

The law which allows for class actions was implemented in Poland recently and there is no case law in this respect. The first cases raised do not refer to personal data processing. Moreover, they show that this legal instrument is not very useful in practice.

10.6 Liability

The data controller is the entity who will be primarily liable for damages resulting from a breach of the PDP. Moreover, with respect to the violation of these provisions of the PDP which regulate the protection of personal data and implementation of appropriate technical and organisational measures for protecting the personal data, the data processor may also be liable.

The liability for damages resulting from a breach of the PDP is based on general principles of Polish civil law, as the PDP does not contain any specific regulations in this respect. In principle, claims for compensation or damages may be based on two legal principles. The first one is the infringement of so-called 'personal interest' of the data subject, which includes, for example, the right to privacy. The data subject whose personal interests where infringed may claim compensation for non-pecuniary 'damage' or claim damages based on general rules. The second basis of the claim is tort liability. Moreover, if the data subject and the data controller were bound by the contract, the data subject may raise claims for damages arising from the breach of such contract.

The claims for damages resulting from a breach of the PDP are not very common. In practice, they usually accompany the claims for compensation for infringement of personal interest. Therefore, it is difficult to identify the precise amount of damages awarded for a breach of the PDP.

Portugal

Coelho Ribeiro e Associados – Sociedade Civil de Advogados R.L Mónica Oliveira Costa

1. LEGISLATION

1.1 Name/title of the law

Law no. 67/98, of 26 October (*Lei de Protecção de Dados Pessoais* – Data Protection Law (DPL)) implements Data Protection Directive 95/46/EC (Directive).

In addition, in particular the following Laws also contain specific rules regarding data protection:

- Law no. 43/2004 of 18 August – approves specific rules concerning the organisation and functioning of the Portuguese Data Protection Authority (*Comissão Nacional de Protecção de Dados*) (CNPD);
- Law no. 7/2009, of 12 February (Portuguese Labour Code);
- Decree-Law no. 134/2009 of 2 June subsequently modified by Decree Law no. 72-A/2010 of 18 June – concerning the legal regime applicable to call centres and phone call recording;
- Law no. 12/2005 of 26 January – laying down the legal framework applicable to personal genetic information and health information;
- Law no. 32/2008 of 17 July – implements Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks;
- Law no. 41/2004, of 18 August – implements Directive 2002/58/EC, of the European Parliament and of the Council, of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive);
- Decree-Law no. 7/2004, of 7 January subsequently modified by Decree-Law no. 62/2009 of 10 March – implementing Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market as well as Article 13 of Directive 2002/58/EC;
- Administrative Rule no. 469/2009, of 6 May, subsequently modified by the Administrative-Law no. 131/2010 of 2 March and last amended by Administrative Rule no. 694/2010, of 16 August – lays down the technical and security conditions under which electronic communications for the transmission of traffic and location data on natural persons and legal entities, as well as of related data necessary to identify the subscriber or registered user, must operate, pursuant to Law no. 32/2008, of 17 July;

- Law no. 34/2009 of 14 July – laying down the legal framework applicable to the processing of data relating to the judicial system;
- Decree-Law no. 35/2004 of 21 February – concerning the use of video surveillance for the protection of people and goods;
- Law no. 1/2005 of 10 January, subsequently modified by Law no. 39-A/2005 of 29 July – on the use of video surveillance by law enforcement authorities in public places;
- Decree-Law no. 207/2005 of 29 November – lays down the installation and data processing procedures of the traffic video surveillance;
- Law no. 51/2006 of 29 August – on the use of video surveillance and other electronic systems to monitor traffic, incidents and infringements on the highways;
- Law no. 33/2007 of 13 August – governing the installation and use of video surveillance systems inside taxis;
- Administrative Law No 314-A/2010 of 14 June – establishing the terms and conditions governing the processing of data obtained by means of electronic identification or detection of vehicles through electronic registration devices;
- Administrative Law No 314-B/2010 of 14 June – establishing the use of electronic registration devices for electronic toll collection.

1.2 Pending legislation

The amendments to the ePrivacy Directive (brought about by Directive 2009/136/EC) have not yet been implemented in the Portuguese jurisdiction, despite the implementation deadline having passed on 25 May 2011.

1.3 Scope of the law

1.3.1 The main players

The main players under the DPL are:

- The 'controller': 'a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data';
- The 'processor': 'a natural or legal person, public authority or any other body which processes personal data on behalf of the controller';
- The 'data subject': 'an identified or identifiable natural person, ie 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';
- The 'third party': 'any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data'.
- The 'recipient': 'a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a law shall not be regarded as recipients'.

1.3.2 Types of data

The DPL applies exclusively to data relating to natural persons and not to data relating to legal persons/companies.

'Personal data' are defined by the DPL as 'any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identifiable natural person ('data subject')'.

The DPL distinguishes three categories of special personal data that are subject to more restrictive processing conditions:

(i) 'sensitive data', ie, 'personal data revealing philosophical or political beliefs, political party or trade union membership, religion, private life and racial or ethnic origin, as well as the processing of data concerning health or sex life, including genetic data' as well as video surveillance; data which are subject to confidentiality; profiling; drug and alcohol testing in the workplace; traffic and location data;
(ii) 'suspicion of illicit activities, criminal and administrative offences and pecuniary sanctions'; and
(iii) 'data concerning credit and solvability', ie, personal data revealing the economic capacity of the data subject in order to evaluate the terms and conditions under which credit can be granted.

1.3.3 Types of acts/operations

The DPL applies to all 'processing' of personal data, defined as being 'any operation or set of operations which is performed upon personal data, whether wholly or partly by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

The DPL shall apply to processing of personal data wholly or partly by automated means, and to processing other than by automated means of personal data which form part of manual filling systems or which are intended to form part of manual filling systems.

'Personal data filing system' shall mean 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis'.

Although non-automated processing and/or manual filing systems fall within the scope of the DPL they are nevertheless subject to the specifications and simplified rules as set out in the CNPD's Guidelines of 15 January 2002. Manual filing systems are exempt of being notified to the CNPD with the following exceptions: (i) processing of sensitive data or suspicion of illegal activities, criminal and administrative offences; and (ii) international transfers.

Furthermore, the DPL shall apply to video surveillance and other forms of capture, processing and dissemination of sound and images allowing people to be identified, provided the controller is domiciled or based in Portugal or makes use of a computer or data communication network access provider established on Portuguese territory.

1.3.4 Exceptions

The processing of personal data by a natural person in the course of a purely personal or household activity falls outside the scope of the DPL.

Moreover, there are partial exemptions on the application of the DPL which exist for certain types of data processing, including manual filing system (in accordance with the CNPD's Guidelines of 15 January 2002), processing by public security services and processing for journalistic, artistic or literary purposes, as far as the right to information of the data subject is concerned.

1.3.5 Geographical scope of application

The DPL shall apply to the processing of personal data carried out:

- in the context of the activities of an establishment of the controller on Portuguese territory;
- outside national territory, but in a place where Portuguese law applies by virtue of international public law (eg, Portuguese embassies); and/or
- by a controller who is not established on the European Union territory and who for the purposes of processing personal data makes use of equipment, automated or otherwise, situated on the Portuguese territory, unless such equipment is used only for the purposes of transit through the territory of the European Union. In this case, the controller must designate a representative domiciled or based in Portugal to replace him in all his rights and obligations, without prejudice to his own liability.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Portuguese Data Protection Authority – *Comissão Nacional de Protecção de Dados* (CNPD)
Rua de São Bento, n.º148, 3.º
1200-821 Lisboa
T: +351 213 928 400
F: +351 213 976 832
Privacy line: +351 213 930 039
E: geral@cnpd.pt
W: *www.cnpd.pt*

The CNPD is an independent body whose main purpose is to monitor and supervise the processing of personal data, while strictly respecting human rights and fundamental freedoms and guarantees as laid down in the Constitution and the law.

In particular, but not limited to, the CNPD can:

- issue prior opinions on legal provisions and instruments in preparation relating to personal data processing;
- authorise or record, as applicable, personal data processing;
- authorise the use of personal data for purposes other than their

collection as well as the interconnection of data and the transfer of personal data outside the EU, when required by law;
- set down the data retention period according to the purpose of processing, issuing guidelines for specific sectors of activity;
- ensure the right of access to personal data and the exercise of the right of rectification and updating.

2.2 Powers

In order to perform all its tasks, the CNPD is endowed with the following powers:
- powers of investigation, having access to data undergoing processing;
- powers of authority, namely ordering blocking, erasure or destruction of personal data, or imposing a temporary or permanent ban on the processing of personal data;
- powers to warn or publicly censure the controller for failure to comply with legal provisions on data protection;
- powers to initiate legal proceedings for breach of the DPL;
- powers to report to the Public Prosecutor Office any criminal offences detected in the scope of its functions and to take all necessary and urgent measures to obtain evidence.

2.3 Priorities

The CNPD draws up an annual report explaining how it has executed its management plan in the preceding year. This report presents an assessment of the international and national activities of the CNPD, including its recommendations, authorisations and resolutions as well as statistical data on proceedings.

The CNPD also adopts an annual plan of activities. In its 2011 plan of activities, approved in January 2011, the CNPD listed its priorities, namely: electronic notification; location data; personal data of minors; reuse of email accounts; new guidelines on monitoring of employees in the workplace: phone calls, email and internet access; and intensification of supervisory action and international intervention in a year marked by the revision of data protection in the European Union and the amendment of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

According to the DPL, as a general rule, in order to process any personal data, the data subject's consent must be obtained.

'Consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

It is the CNPD's understanding that 'freely' means that the data subject's will is not affected in any way; 'specific' means that it refers to a precise and

limited operation; 'informed' means that the data subject is fully aware and understands all the aspects of the processing and that the consent can be withdrawn by the data subject at any time.

3.1.2 Form

The DPL does not require consent to be given in a specific form. However, for the processing of health data, it must be in writing and for clinical trials written consent should comply with a template drafted by the controller applicable to all data subjects that will be subject to clinical trials. For the processing of sensitive data, consent must be explicit, which means that the data subject must authorise the processing of sensitive data, ie, it cannot be inferred or extracted from other statements as if implicitly stated therein.

3.1.3 In an employment relationship

It is debatable whether consent can be considered to constitute a legal ground for the processing of employees' personal data by the employer due to the subordinate position of the employee in the employment relationship in which the employee might not be considered to be truly 'free'. Therefore, when evaluating the legitimacy of data processing in an employment relationship, the CNDP may not deem the employee's consent to be sufficient if the processing relies solely on it.

In the last amendment to the Labour Code in 2009, the legislator withdrew the possibility for the employee to consent to the disclosure of his health data to the employer.

3.2 Other legal grounds for data processing

Personal data, except for the categories of special personal data described in section 1.3.2 above, may also be processed under the DPL if necessary:

- for the performance of a contract or contracts to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his will to negotiate;
- for compliance with a legal obligation to which the controller is subject;
- in order to protect the vital interests of the data subject if the latter is physically or legally incapable of giving his consent;
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

Processing sensitive data is prohibited unless:

- processing is essential for the controller to exercise his legal or statutory rights in view of a relevant public interest; or
- the data subject explicitly gives consent.

In both cases, guarantees of non-discrimination and security measures provided for in DPL are also required (see section 9 below).

Furthermore, the processing of sensitive data under the DPL is also allowed in the following cases:

- when it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
- when it is carried out with the data subject's consent in the course of its legitimate activities by a foundation, association or non-profit seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
- when it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations;
- when it is necessary for the establishment, exercise or defence of legal claims and is exclusively carried out for that purpose.

Processing of data relating to health and sex life, including genetic data, shall equally be permitted if necessary for the purposes of:

- preventive medicine;
- medical diagnosis;
- provision of care or treatment; or
- management of health-care services.

In all the above health and sex life processing cases, data must be processed by a health professional bound by professional secrecy or by another person subject to an equivalent obligation of secrecy and adequate safeguards must be in place.

Under certain circumstances, the processing of health data is also allowed for the following purposes:

- scientific research (CNPD's guidelines of 28 May 2007);
- clinical trials (CNPD's guidelines of 16 July 2007);
- pharmacovigilance (CNPD's guidelines of 16 March 2009).

And finally, in an employment relationship, processing of health data is allowed for the following purposes:

- preventive and curative medicine in testing drug and alcohol at the workplace (CNPD's guidelines of 15 November 2010);
- health and safety at work (CNPD's guidelines of 11 October 2010).

The processing of personal data related to people suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties is only allowed if undertaken by public services and under the terms laid down by law.

The processing of credit and insolvency data is only allowed in the following cases:

- if it can be legally foreseen (eg, legal framework of credit institutions and financial companies);
- with consent from the data subject; or

- under a contractual clause included in an agreement between the debtor and the creditor.

Notwithstanding this, processing may also be authorised by the CNPD, when it is necessary for pursuing legitimate purposes of the controller, provided the fundamental rights and freedoms of the data subject are not overridden and the security of information rules are safeguarded.

3.3 Direct marketing and cookies

The data subject has the right to be informed before personal data are disclosed for the first time to third parties for the purpose of direct marketing or for their use on behalf of third parties.

Additionally, the data subject has the right to object, on request and free of charge, to the processing of his personal data for purposes of direct marketing or any other form of research.

Furthermore the data subject shall be expressly offered the right to object to such disclosure or uses free of charge.

As far as direct marketing is concerned, the provisions of Decree-Law no. 7/2004, of 7 January (which implemented Directive 2000/31/EC as well as Article 13 of Directive 2002/58/EC), must also be taken into account.

Portugal adopted two different systems:

- opt-in for natural persons, with a derogation whenever there has been previous transactions regarding the same or similar products/services and provided that they had explicitly been given the opportunity to object to such messaging at that time;
- opt-out for legal persons.

In any case, the recipient must be granted access to the appropriate means that enables the refusal, at any time, of future communications, freely and without cause. Moreover, each unsolicited communication shall indicate an address and an electronic technical means, easy to identify and to use, which allows the recipient of the service to object to future communications.

In addition, it should be noted that the law prohibits the practice of sending electronic mail for the purposes of direct marketing while disguising or concealing the identity of the person on whose behalf the communication is made.

Finally, the entities that undertake the sending of certain unsolicited advertising communications shall maintain, on their own or through the entities that represent them, an updated list of persons who have expressed their wish not to receive such advertising communications. In 2009, a public list, updated on a quarterly basis, of whoever expressed their wish not to receive such advertising communications, was created. Therefore, since 9 May 2009, the entities which undertake this activity have a double mandatory task: (i) to maintain and update their personal lists; (ii) and to consult the public list on a regular basis, no less than once every quarter.

The sending of advertisement communications by electronic means to the people included in such lists is forbidden.

With regard to cookies, since the amendments to the e-Privacy Directive have not yet been implemented in Portuguese law, their use is still governed

by the previous opt-out system requiring that the user has been given clear and comprehensive information, namely on the purpose of the processing. Nevertheless, the use of cookies will always be permitted if necessary to:

- carry out or facilitate the transmission of a communication on an electronic communications network; or
- provide a service within the scope of the information society that has been explicitly requested by the subscriber or by any user.

3.4 Data quality requirements

Personal data must be:

- processed lawfully and with respect for the principle of good faith;
- collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, when necessary, kept up to date – adequate measures must be taken to ensure that data which are accurate were collected or for which they are further processed, are erased or rectified; and
- kept in a form that allows identification of the data subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed.

3.5 Outsourcing

According to the DPL, any person acting under the authority of the controller or the processor, including the processor himself, who has access to personal data shall only process data upon instructions from the controller and on his behalf, unless he is required to do so by law.

The controller must choose a processor capable of ensuring technical security and adopt organisational rules on the processing to be carried out, and is responsible for the processor's compliance with those rules.

In addition, the carrying out of processing by way of a processor must be governed by a contract or other legal act which shall expressly lay down that the processor shall act only upon instructions from the controller and that it must adopt all measures required by law to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

3.6 Email, internet and video monitoring

3.6.1 General rules

Email, internet and video monitoring are subject to the provisions of the DPL, Law no. 41/2004, of 18 August on the protection of privacy in the electronic communications sector), the Portuguese Labour Code (Law no. 7/2009, of 12 February), Decree-Law no. 35/2004 of 21 February (on the use of video surveillance for the protection of people and goods), Law no. 1/2005 of 10 January, (on the use of video surveillance by law enforcement authorities in public places) and Decree-Law no. 207/2005 of 29 November (on the installation and data processing procedures of traffic video surveillance).

In addition, the CNPD has also issued Guidelines on CCTV surveillance (19 April 2004) as well as on the monitoring of employees in the workplace – phone calls, email and internet (29 October 2002).

Email, internet and video monitoring require prior authorisation from the CNPD. The use of video surveillance by law enforcement authorities in public places is subject to the previous opinion of the CNPD.

It is worth mentioning that the CNPD has also issued guidelines on the following subjects:

- use of biometric data in controlling access and monitoring employees' attendance (26 February 2004); and
- telephone call recording to monitor the quality of contact services (13 September 2010).

3.6.2 Employment relationship

Email and internet monitoring must be covered by a company policy paper laying down the terms and conditions for the use of electronic means for private purposes and the consequences in case of any misuse, as well as the monitoring methods adopted with respect to the employee's privacy and without resorting to abusive and disproportionate means of control. The policy must be submitted to the opinion of the workers' council and registered with the Labour Authority as well as advertised in the workplace so that all employees are made aware of its contents. Monitoring shall be carried out generally, instead of focusing on individual employees, and on a non-regular basis.

The purpose of monitoring emails shall be to guarantee the security of the systems and the performance, as well as the prevention or detection of disclosure of trade secrets, in which case only the employees with access to those secrets when there are grounds for suspicion, shall be monitored.

When accessing the employee's email, which should always be a procedure of last resort, the employee should be present, and he or she is entitled to indicate which emails are private and therefore not accessible to the employer.

As far as the internet is concerned, monitoring shall be based on the amount of time spent on the web, and the most frequently accessed websites.

The use of video surveillance in the workplace will only be allowed for the purpose of guaranteeing the safety of people and goods or whenever the type of work justifies its use, provided that there are no other less intrusive methods capable of achieving the same results. CCTV cannot be used to monitor the work performance of employees.

The use of video surveillance is subject to the prior opinion of the works' council and requires putting up notices informing people that the CCTV is being used.

4. INFORMATION OBLIGATIONS

4.1 Who

Controllers are responsible for informing data subjects about the processing of their personal data.

4.2 What

Unless the data subject is already aware of the following, the controller under the DPL must provide the following information to the data subject:

- the identity of the controller and of his representative, if any;
- the purpose(s) of the data processing;
- other information such as: the recipients or categories of recipients; whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply; and the existence and conditions of the right of access and the right to rectify; and
- that personal data, when collected in open networks, may circulate without security measures and may be at risk of being seen and used by unauthorised third parties.

Specific information may be required based on the nature of the processing.

4.3 When

The abovementioned information should be provided when recording the data or, in case of them being disclosed to third parties, no later than the date on which the data are first disclosed.

4.4 How

The DPL does not specify in which form and how the information must be provided. Nevertheless, if the collection is made by means of a document, this document should contain the above mentioned information.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Upon request, every data subject under the DPL has the right to:

- know if his data are being processed as well as the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed.
- get information concerning the data processed and any available information as to their source; and
- be informed of the logic involved in any automatic processing of his data.

Data access may also be obtained through the CNPD (regarding judicial data, criminal investigation, national security as well as processing of journalistic, artistic or literary data) and, in the case of health data, from the physician chosen by the data subject.

Access to third party data (eg, by family of the deceased patients) as far as health data are concerned is regulated by the CNPD Guidelines of 3 July 2001 and 30 May 2006.

5.1.2 Exceptions

There are no derogations from the right of access for the data subjects, although, when legally foreseen, the right of access can be restricted

(provided that there is clearly no risk of breaching the right to privacy of the data subject) when the data are:

- used solely for purposes of scientific research; or
- kept for a period which does not exceed the period required for the sole purpose of creating statistics.

5.1.3 Deadline

The data subject can exercise the right to access at any time. The controller must reply without undue delay.

5.1.4 Charges

The data subject may not be charged for exercising his right to access.

5.2 Rectification

5.2.1 Right

The data subject has the right to require and obtain data rectification whenever such data are incomplete or inaccurate, and also to require notification of any rectification to third parties to whom the data may have been disclosed, unless such notification proves to be impossible.

5.2.2 Exceptions

There are no derogations from the right to rectification.

5.2.3 Deadline

The controller should rectify the personal data without undue delay. For the direct marketing sector and under their Code of Conduct, the rectification should be made within 30 days.

5.2.4 Charges

The data subject may not be charged for exercising his right to rectification.

5.3 Erasure

5.3.1 Right

Any data subject has the right to obtain the erasure of all personal data relating to him if:

- the data are incomplete or irrelevant for the purpose of the processing;
- recording, disclosure or storage of the data is prohibited; or
- the data have been stored for longer than the permitted retention period.

5.3.2 Exceptions

There are no derogations from the right to erasure.

5.3.3 Deadline

The controller should erase the data without undue delay. For the direct marketing sector and under their Code of Conduct the rectification should be made within 120 days at the very latest.

5.3.4 Charges

The data subject may not be charged for exercising his right to erasure.

5.4 Blocking

5.4.1 Right

Any data subject has the right to block any use of personal data relating to him under the same conditions as the right to erasure.

5.4.2 Exceptions

There are no derogations from the blocking right.

5.4.3 Deadline

The DPL does not set a deadline for exercising the blocking right.

5.4.4 Charges

The data subject may not be charged for exercising his blocking right.

5.5 Objection

5.5.1 Right

The data subject has the right to object to the processing of personal data, at any time, on compelling legitimate grounds, unless otherwise provided for by law.

Moreover, the data subject has the right to object to the processing of his personal data for direct marketing purposes or for any other form of research, on request and free of charge.

5.5.2 Exceptions

The data subject does not have the general right to object to the processing of his personal data if it is deemed necessary for the performance of legal or contractual obligations of the controller, provided that in this case that the data subject is party to the said contract.

5.5.3 Deadline

If the data subject objects to the processing of personal data, the controller must reply without undue delay. If the objection is legitimate or is made based on direct marketing purposes, the controller must immediately cease to process the personal data.

5.5.4 Charges

The data subject may not be charged for exercising the right to object.

5.6 Automated individual decisions

5.6.1 Right

The data subject has the right not to be subjected to a decision affecting him as a result of automated data processing aimed at evaluating certain aspects of his personality, in particular his performance at work, creditworthiness, reliability or conduct.

5.6.2 Exceptions

The right does not apply if:

(i) that decision is taken in the context of a contractual relationship;

(ii) adequate measures to safeguard the data subject's legitimate interests have been taken, particularly mechanisms allowing him to express his point of view; or

(iii) if authorised by the CNPD, provided that it is based on measures to safeguard the data subject's legitimate interests.

5.6.3 Deadline

The DPL does not set any specific deadline for this matter.

5.6.4 Charges

The data subject may not be charged for exercising his right.

5.7 Other rights

5.7.1 Right

The data subject also has the right to require from the controller that his data are collected lawfully; are not disclosed to third parties without his prior knowledge; and are not processed for purposes other than those for which they were collected in the first place.

5.7.2 Exceptions

There are no derogations.

5.7.3 Deadline

There is no deadline.

5.7.4 Charges

The data subject may not be charged for exercising this right.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The responsibility for notifying personal data processing to the CNPD lies with the controller.

6.1.2 What

As a general rule, any wholly or partly automated processing operation, or set of such operations, intended to serve a single purpose or several related purposes is subject to prior notification. The CNPD has published guidelines on the notification requirements and exemptions on its website.

Each purpose for which personal data are processed, or each group of connected purposes, requires a separate notification.

6.1.3 Exceptions

A processing activity is exempt from notification if its sole purpose is to

keep a register which according to laws or regulations is intended to provide information to the public and which is open to consultation by the general public or to any person demonstrating a legitimate interest.

In addition, personal data processing is also exempt from notification to the CNPD if its purpose is one of the following:

- payroll management;
- staff management;
- clients', suppliers' and service providers' invoicing and contact management;
- buildings access control (entries and exits);
- collection of an association's contributions and contact administration of its members;
- management of library and archive users.

The notification exemption applies only if the terms and conditions established by the CNPD for such exemption are met, such as the type of data processed, the purpose of processing and the time during which the data may be stored, provided that no international transfers occur.

6.1.4 When

Notification must be made prior to starting any automated processing activity as well as any changes to it.

6.1.5 How

The CNPD implemented the electronic notification form in January 2011. As a general rule, the CNPD will no longer accept paper forms. Thus, whenever possible, notifications should be submitted online by filling in the relevant form in Portuguese. The CNPD has more than one form depending on the purpose of the processing. The notification form includes information, among others, on the identification of the controller and processor (if applicable), the processing purpose and the categories of the personal data processed as well as the recipients of the data, international transfer, retention period, etc.

Upon payment of the notification fees, the controller may start the notified processing activity, unless prior authorisation is required. The CNPD is however entitled to request additional information from the controller.

6.1.6 Notification fees

The fees for processing notifications have been updated. If the processing is subject to prior authorisation, a fee of €150 will apply, if not, it will cost €75.

However, when notifications are particularly complex, the CNPD may increase the fee by half of the national minimum salary in force, which, in 2011, amounts to a maximum of €242.50.

The fee for electronic notification must be paid within three working days of submitting the electronic form and afterwards the payment confirmation shall be sent to the CNPD.

6.2 Authorisation requirements

6.2.1 Who

The responsibility for request authorisation for personal data processing to the CNPD lies with the controller.

6.2.2 What

According to Opinion no. 50/2011, issued last January by the CNPD, authorisation is required, among others, for:

- processing sensitive data;
- processing personal data relating to people suspected of illegal activities, criminal and administrative offences and decisions applying penalties, security measures, fines and additional penalties;
- processing personal data relating to credit and the solvency of the data subjects;
- combining personal data (ie a form of processing which consists of the possibility to correlate data in a filing system with data in a filing system or systems kept by another or other controllers or kept by the same controller for other purposes);
- use of personal data for purposes not originally giving rise to their collection;
- transfer of personal data to a state which does not guarantee an adequate level of protection;
- processing of biometric data; and
- issuing notifications to extend the retention period of personal data for historical, statistical or scientific purposes.

6.2.3 Exceptions

Not applicable.

6.2.4 When

Authorisation must be granted by the CNPD before starting any automated processing activity as well as any changes to it.

6.2.5 How

The same procedure as referred to in section 6.1.5 above.

6.2.6 Authorisation fees

See section 6.1.5 above.

6.3 Other registration requirements

Not applicable.

6.4 Register

The CNPD holds a public register of notified processing operations. Recently the content of the decisions was made publicly accessible on the CNPD website and searching by controllers' name as well as keywords is available.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Under the DPL, it is not mandatory to appoint a data protection officer.

7.2 Tasks and powers

Not applicable.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Data transfers from Portugal to other EU member states are not subject to any additional requirements, as those countries are deemed to provide an adequate level of protection. The same applies to countries outside the EU which have been officially recognised by the European Commission as providing an adequate level of protection.

The transfer of personal data which are undergoing processing or are intended for processing to a state which is not a member of the EU or considered adequate, may only take place subject to compliance with the DPL and provided the state to which they are transferred ensures an adequate level of protection.

The adequacy of the level of protection of a state outside the EU shall be assessed by the CNPD in the light of all the circumstances surrounding a data transfer (including the nature of the data; the purpose and duration of the proposed processing transactions; the exporting and importing countries; the law; professional rules and security measures of the state to which the data are transferred). It is up to the CNPD to decide whether a state outside the EU ensures an adequate level of protection.

8.2 Legal basis for international data transfers

The transfer of personal data to a state that does not ensure an adequate level of protection is allowed if the transfer:

- is unambiguously consented to by the data subject;
- is necessary for the performance of an agreement between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;
- is necessary for the performance or conclusion of an agreement concluded or to be concluded in the interests of the data subject between the controller and a third party;
- is necessary or legally required on important public interest grounds, or for the establishment, exercise of defence or legal claims;
- is necessary in order to protect the vital interests of the data subject;
- is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

In accordance with the CNPD's guidelines of 29 November 2004, none of the above described cases require authorisation by the CNPD, although they

be should expressly referred to in the notification to the CNPD.

8.2.1 Data transfer agreements

The CNPD may authorise a transfer or a set of transfers of personal data to a state which does not ensure an adequate level of protection, provided that the controller guarantees adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses.

If the transfer is made using the European Commission's standard contractual clauses, no authorisation from the CNPD will be required, although it needs to be expressly referred to in the notification to the CNPD.

8.2.2 Binding corporate rules

The CNPD is of the opinion that binding corporate rules (BCRs) are not enforceable in Portugal and therefore cannot give rise to obligations. The CNPD does not accept BCRs as a means of legitimising transfers of data to countries outside the EU.

8.2.3 Safe Harbour

Transfer of personal data to an entity that is certified under the US Safe Harbour scheme is not subject to authorisation by the CNPD, provided that the data transfer falls within the scope of the US Safe Harbour certification and it is expressly referred to in the notification to the CNPD.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The DPL requires that all controllers, processors and in general all persons who obtain knowledge of the personal data processed in the course of carrying out their functions as well as after their functions have ended shall ensure the confidentiality of personal data, and are bound by professional secrecy.

9.2 Security requirements

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

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks incurred by the processing and the nature of the data to be protected.

Notwithstanding the need for the processor to implement appropriate technical and organisational measures, the controller is always responsible for ensuring compliance by the processor with those measures.

Special security measures should be taken by the controller when processing any of the three categories of special personal data described

above in section 1.3.2 above. Moreover, it is also required that the systems guarantee a clear separation between data relating to health and sex life, including genetic data, from other personal data.

In some circumstances the CNPD may also request that the transmission of data be encoded.

9.3 Data security breach notification obligation

Currently, there is no obligation to notify personal data security breaches to the data subjects and/or to the CNPD.

9.4 Data protection impact assessments and audits

There is no general requirement to carry out data protection impact assessments and audits under Portuguese law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The CNPD is responsible for assessing claims and complaints from individuals. Furthermore, the CNPD may conduct an investigation and may have access to data undergoing processing and has powers to collect all the information necessary for the performance of its supervisory role.

The CNPD may also carry out targeted inspections on its own initiative as well as on-site investigations during which the controller must provide all necessary information upon request and fully co-operate with the CNPD.

In addition, the CNPD may issue opinions and recommendations, either on its own initiative, or at the request of government and legislative bodies, on any matter relating to the protection of privacy and personal data.

10.2 Sanctions

The processing of personal data in breach of the DPL may constitute an administrative offence subject to fines of €30,000 maximum.
Nevertheless the amount may increase up to a maximum of:

- €66,666.66 for any breach of the direct marketing rules (see section 3.3 above); and
- €5,000,000 for any breach of the processing of personal data and the protection of privacy in electronic communications, including cookies (see section 3.3 above).

The CNPD is empowered to levy fines provided in the DPL, in the name of its chairman and these fines shall be enforceable if they are not challenged.

Moreover, the processing of personal data in breach of the DPL may also constitute a crime penalised with a maximum of four years' imprisonment or a fine of a maximum of 480 days.

The CNPD is not empowered to investigate any criminal offences and shall report them to the Public Prosecutor's Office and take all necessary and urgent measures to provide evidence.

In addition to the abovementioned fines and penalties, the CNPD or the court may take the following measures:

- temporary or permanent prohibition of processing;
- blocking, erasure or total or partial destruction of data;
- publication of the decision or sentence;
- public warning or censure of the controller.

10.3 Examples of recent enforcement of data protection rules

According to the CNPD 2010 activities report, in 2010, the CNPD carried out 189 inspections, deliberated on 863 misdemeanour cases and levied 248 fines.

10.4 Judicial remedies

Without prejudice to the right to lodge a complaint to the CNPD, according to the law, any individual may have recourse to administrative and legal means to guarantee compliance with the legal provisions in the area of personal data protection.

The CNPD's decisions are binding and are subject to appeal to the Central Administrative Court. In the case of administrative offences, the decisions of the CNPD may be appealed to the criminal courts.

In Portugal, employment disputes as well as appeals against the CNPD's decisions regarding CCTV are the most common judicial proceedings concerning privacy and data protection.

10.5 Class actions

The right of *actio popularis* is a constitutional right, either personally or via associations that purport to defend the interests in question and under the terms provided for by law, including the right to apply for the applicable compensation for an aggrieved party or parties, in order to, for instance:

- promote the prevention, cessation or judicial prosecution of offences against public health, consumer rights, the quality of life or the preservation of the environment and cultural heritage;
- safeguard the property of the state, the autonomous regions and the local authorities.

Hitherto, there is no record in Portugal of any relevant *actio popularis* concerning privacy and data protection.

10.6 Liability

The controller shall be held liable for any damage as a result of an action in violation of the provisions of the DPL.

Any person who has suffered damage as a result of an unlawful processing operation or of any other act incompatible with legal provisions in the area of personal data protection is entitled to receive compensation from the controller for the damage suffered.

However, the controller may be exempted from this liability, wholly or partly, if he can prove that he is not responsible for the event giving rise to the damage.

In November 2010, the Évora Court of Appeal decided that although CCTV cannot be used to monitor the performance of employees at work, images taken of employees can be used as evidence in disciplinary

proceedings provided that the employer is authorised by the DPA to use CCTV for the purpose of the protection of persons and property, and the employee's conduct as revealed by the CCTV images is contrary to it.

Finally, in February 2011, the Southern Central Administrative Court, in injunction proceedings, confirmed the decision of the DPL, which refused to authorise the City Council of Lisbon to install CCTV for traffic control purposes in order provide assistance to victims of car accidents. The court held that the cameras were equipped with zoom and rotation mechanisms that would enable the taking of images that have nothing to do with traffic control, including images of the licence plates of parked vehicles, demonstrations or public meetings, and even of the private lives of residents in surrounding buildings. The CCTV capabilities therefore clearly exceeded the purpose for which they were intended. Furthermore, less privacy-intrusive measures could be adopted by the City Council, which would be sufficiently effective, eg, policing.

Republic of Ireland

Mason Hayes & Curran Jeanne Kelly & Aoife Treacy

1. LEGISLATION

1.1 Name/title of the law

The main law governing the collection and processing of personal data in Ireland is the Data Protection Act, 1988, the object of which was to give effect to the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data. This was subsequently modified by the Data Protection (Amendment) Act, 2003 which implemented the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Directive). The Data Protection Act, 1988 and the Data Protection (Amendment) Act, 2003 are cited as the Data Protection Acts, 1988-2003 (together here called the DPA).

Ireland has also enacted secondary data protection legislation, the most important of which gives effect to the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive) (as amended). These are entitled the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 SI 336 of 2011 (the 2011 Regulations).

Finally, the Irish courts have held that the Constitution of Ireland, 1937 provides for an implicit constitutional right to privacy under Article 40.3.

1.2 Pending legislation

Currently, there is no important data protection legislation pending in Ireland. There is some which may have an indirect impact, such as the Whistleblowers Protection Bill 2011 which was presented to the Irish Parliament in June 2011. The purpose of this bill is to provide protection from civil liability to employees who make certain disclosures 'reasonably and in good faith' in relation to the conduct of the business and affairs of their employers. The bill lists the Data Protection Commissioner (DPC) as one of the chief regulatory authorities of Ireland to whom disclosures may be made.

The compatibility and implications of whistleblowing schemes with data protection principles have been considered in depth by the Article 29 Working Party in its Opinion on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fighting against bribery, banking and financial crime (WP 117).

However, as the bill is at a preliminary stage it is not possible to comment

on the nature or extent of the effect that the legislation will have on the data protection laws in Ireland.

1.3 Scope of the law

1.3.1 The main players

- the 'data controller' is a person who, either alone or with others, controls the contents and use of personal data;
- the 'data processor' is a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment;
- the 'data subject' is an individual who is the subject of personal data;
- 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the data controller, the data processor and the persons who, under the direct authority of the data controller or the data processor, are authorised to process the data.

1.3.2 Types of data

The DPA regulates the processing of 'personal data'. 'Personal data' are 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. Data relating to companies do not come within the remit of this definition.

The DPA distinguishes between 'personal data' and 'sensitive personal data'. Processing of the latter is subject to more stringent pre-conditions than the former. 'Sensitive personal data' means personal data as to:

(a) racial or ethnic origin;
(b) political opinions;
(c) religious or philosophical beliefs;
(d) trade union membership;
(e) physical or mental health or condition or sexual life;
(f) commission or alleged commission of an offence; or
(g) proceedings for an offence committed or alleged to have been committed.

1.3.3 Types of acts/operations

The DPA regulates the 'processing' of personal data. Section 1 broadly defines this as the performing of any operation or set of operations on the data, whether or not by automatic means, including:

(i) obtaining, recording or keeping the information, or data;
(ii) collecting, organising, storing, altering or adapting the information or data;
(iii) retrieving, consulting or using the information or data;
(iv) disclosing the information or data by transmitting, disseminating or otherwise making them available; or
(v) aligning, combining, blocking, erasing or destroying the information or data.

'Data' under the DPA include both automated and manual data, which are processed as part of a relevant filing system. A 'relevant filing system'

means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

1.3.4 Exceptions

Personal data contained in disorganised paper documents will not fall under the DPA.

In addition, the following specific cases fall outside the remit of the DPA:

- personal data that in the opinion of the Minister for Justice or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the Irish state;
- personal data consisting of information that the person keeping the data is required by law to make available to the public; or
- personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes.

There are also exceptions provided for the restrictions on the processing of personal data. These include, where the processing is:

- required for the purpose of safeguarding the security of the state in the opinion of a member of the Irish Police Force or an officer of the Permanent Defence Force (of certain ranking) designated by the Minister for Defence;
- required for the purpose of investigating offences where the restrictions would be likely to prejudice this;
- required in the interests of protecting the international relations of the state;
- required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
- required by or under any enactment or by a rule of law or order of a court;
- required for the purposes of obtaining legal advice/in the course of legal proceedings; or
- made at the request or with the consent of the data subject (or his/her nominee).

Note that these exceptions do not apply to the entire scope of the DPA, for example, the right of access still applies to the above situations.

Finally, certain provisions of the DPA (see section 3 below) do not apply to:

- data kept solely for the purpose of historical research; or
- other data consisting of archives or departmental records, the keeping of which comply with such requirements (if any) as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects.

1.3.5 Geographical scope of application

The DPA only applies to data controllers in respect of processing personal data if:

- the data controller is established in the state of Ireland and the data are processed in the context of that establishment; or
- the data controller is established neither in the state of Ireland nor in any other member state of the European Economic Area (EEA) but makes use of equipment in the state of Ireland for processing the data otherwise than for the purpose of transit through the territory of Ireland.

The definition of 'established in the state' includes an individual who is normally resident in Ireland, a body incorporated under the law of Ireland and a partnership or other unincorporated association formed under the law of Ireland.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Data Protection Commissioner (*An Coimisinéir Cosanta Sonraí*)
Canal House, Station Road
Portarlington
Co. Laois
Ireland.
T: +353 57 868 4800
F: +353 57 868 4757
E: info@dataprotection.ie
Web: *www.dataprotection.ie*

2.1 Role and tasks

Article 9 of the DPA establishes the Data Protection Commissioner (DPC) as the data protection supervisory authority of the Republic of Ireland. The Commissioner is appointed by government and is independent in the exercise of his or her functions. The current DPC is Billy Hawkes. The DPC and his office are responsible for the supervision and enforcement of the provisions of the DPA. In addition to this, the DPC is also responsible for the dissemination of information relating to European Commission decisions on extra-EEA transfers of personal data.

2.2 Powers

The DPA endows the DPC with very broad powers in both the supervision of the DPA and the manner in which he can enforce its provisions.

The DPC may instigate an investigation on receipt of a complaint of a DPA breach or where he is of the opinion that such a breach occurred.

The DPC has the power to request information or enforce compliance with the DPA by issuing respectively 'information notices' or enforcement notices as described in section 10 below.

The DPC has the power to prohibit the transfer of personal data outside

the Irish state. This is done by way of a written notice, termed a 'prohibition notice' to either the data controller or the data processor.

The DPC can prosecute offences and breaches under section 30 of the DPA. He also has the powers to prosecute in relation to offences under the 2011 Regulations.

The DPC has the power to draft codes of practice to assist bodies representing categories of data controllers to apply the DPA in their particular sector. To date, four codes of practice have been approved: one for the *Garda Síochána* (the Irish police force); one for the national personal injuries board; one for the insurance sector; and a final general code in relation to personal data security breach.

2.3 Priorities

In the 2010 annual report, the Office of the DPC underlined the need for accountability on the part of public and private sector organisations for the personal data entrusted to them. One such sector where this was evident was the insurance sector. The extent and proportionality of data sharing in the public sector was also highlighted as a source of concern. It also expressed concern over the use of biometric time and attendance systems as a method of supervising employees and asserted that the DPC would be taking a firm stance in relation to the use of such systems in the future.

3. LEGAL BASIS FOR DATA PROCESSING

Section 2A of the DPA requires that at least one of a set of prescribed pre-conditions be satisfied before a data controller can legitimately process personal data. These pre-conditions include where:

- The data subject has consented to the processing or, if the data subject lacks capacity, consent has been given on his/her behalf by a family member.
- The processing is necessary:
  - (i) for the performance of a contract;
  - (ii) in order to take steps at the request of the data subject prior to entering into a contract;
  - (iii) to ensure compliance with a legal obligation to which the data controller is subject, other than imposed by contract;
  - (iv) to prevent damage to the health or property of the data subject where the seeking of consent may result in his/her vital interests being damaged;
  - (v) for the administration of justice;
  - (vi) for the performance of a statutory function;
  - (vii) for the performance of a function of the government or a government minister; or
  - (viii) for the performance of any other function of a public nature performed in the public interest.
- The processing is necessary for the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular

case by reason of prejudice or the fundamental rights and freedoms or legitimate interests of the data subject.

However, if the data being processed constitute 'sensitive personal data' then additional pre-conditions set out in section 2B must be met. In other words, the provisions of section 2 and one of the pre-conditions under section 2A above must be met in conjunction with one of the following pre-conditions under section 2B:

- the data subject has explicitly consented;
- the processing is necessary under employment law;
- the processing is necessary to prevent injury or serious property damage to the data subject or another person or to protect their vital interests where consent cannot be obtained, or where it is not reasonable to expect the data controller to get such consent or, where the damage or injury will be suffered by a third party, the data subject is unreasonably withholding consent;
- the processing is carried on in the course of the legitimate activities of a non-profit organisation;
- the processing is carried on by political parties or election candidates for the purpose of compiling data on political opinions;
- the processing is authorised by the Minister for Justice, Equality and Law Reform; or
- the processing is necessary:
  - (i) for the administration of justice;
  - (ii) for the performance of a statutory function;
  - (iii) for the performance of the functions of the government or a government minister;
  - (iv) to obtain legal advice, to establish the existence of legal right or in connection with legal proceedings;
  - (v) for medical purposes;
  - (vi) for statistical purposes under the Statistics Act, 1993;
  - (vii) for taxation purposes; or
  - (viii) for calculating social welfare benefits.

3.1 Consent

3.1.1 Definition

The DPA does not provide a definition for consent, however, consent must be interpreted in light of the Directive which defines consent as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

Finally, section 2B of the DPA states that the consent must be explicit. This means that a data subject must be aware of and understand the purposes for which his/her data are being processed.

3.1.2 Form

There is no specific format prescribed for the consent. However the consent must be an informed one in order for the data to be fairly processed. The

DPA provides that this will not occur unless the data subject is provided with certain information. This includes:

- the identity of the data controller;
- the identity of a nominated representative of the data controller, if applicable;
- the purpose(s) for which the data are intended to be processed; and
- any other information which is necessary to enable processing in respect of the data to be fair to the data subject.

Explicit consent, for the purposes of section 2B of the DPA, need not require a data subject to sign a form in all cases. The DPC has commented that consent can be understood to be explicit where a person volunteers personal data after the purposes for the data processing have been clearly explained.

3.1.3 In an employment relationship

The Article 29 Working Party has consistently held, and the DPC has had frequent regard to its opinions, that consent is freely given in circumstances where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment.

There is, therefore, a real concern that the provision of consent in an employment context by an employee may not be legally valid unless the employee can withhold his/her consent without suffering any detriment. In practice, this can be difficult to achieve.

3.2 Other legal grounds for data processing

These are outlined in section 3 above.

3.3 Direct marketing and cookies

The direct marketing and cookies regime has recently been overhauled in Ireland. This is now set out in the 2011 Regulations which came into effect on 1 July 2011. The Regulations set down differing sets of rules to apply to phone, fax, text message and email direct marketing. For example, in respect of unsolicited calls for direct marketing purposes, the Regulations provide that a person may not make them where:

- the user has notified the person that the user does not consent to the receipt of such calls; or
- the user has recorded its objection to the receipt of such calls in the National Directory Database.

Less restrictive provisions apply in the case of direct marketing of individuals who are customers. In this case, the following information must be provided:

- in the case of a call, the name of the person making the call and on whose behalf the call is made;
- in the case of a fax or automated calling machine communication, the name, address and telephone number of the person making the communication (and the same details of the person on whose behalf the call is being made);

- in the case of an email, a valid address at which that person may be contacted.

The use of cookies is also governed by the Regulations. The main change introduced under this legislation is the introduction of a consent requirement. Prior to this, a website user simply had to be provided with the relevant information and given an opportunity to 'opt-out'. Now the user must give positive consent to use of the cookie ('opt-in'). The Regulations provide that consent may be considered given by the use of appropriate browser settings or other technological applications set to accept cookies.

3.4 Data quality requirements

Section 2(1) of the DPA lays down the general data protection principles which are to be abided by in the collection, processing, keeping, use and disclosure of personal data. The following requirements are imposed on data controllers:

- data must be fairly obtained and fairly processed;
- data must be accurate and complete and kept up to date;
- data must have been obtained for one or more specified and legitimate purposes and will not be processed in a manner incompatible with that/these purposes;
- data will be adequate, relevant and not excessive in relation to the purpose for which they were collected or processed;
- data shall not be kept for longer than necessary; and
- appropriate security measures shall be taken against unauthorised access to or processing of, the data, particularly where this involves the transmission of data over a network.

3.5 Outsourcing

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must 'ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form' and stipulating, in particular, the following conditions:

- the data processor shall carry out processing only on and subject to instructions of the data controller; and
- the data processor complies with appropriate security measures against unauthorised access to and unlawful processing of the data.

The data controller is obliged to include these conditions in any contract with the data processor. In addition, it must ensure that the data processor complies with these requirements by obtaining sufficient guarantees in respect of the technical security measures and organisational measures governing the processing and must take reasonable steps to ensure compliance with those measures.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email, internet or surveillance by video cameras involves the processing of personal data, and as such, falls within the scope of the

DPA. The same data protection principles apply once personal data are being processed through these media. As a general rule of thumb, the use of these media to record data without an individual's consent is considered unlawful.

3.6.2 Employment relationship

The DPC specifically endorsed the Article 29 Working Party Opinion on the surveillance of electronic communications in the workplace (WP 55).

Pursuant to this, employees subject to any form of monitoring should know exactly what information about them is being monitored and collected and the extent of the monitoring. In the employment context, the information generally should be more transparent and up-front.

The DPC has stated that 'on-going monitoring is never considered proportionate and access should be in response to a reasonable suspicion'. Consequently, any company or individual engaging in the monitoring of employee data would accordingly need to be able to demonstrate very clearly that this was the least intrusive means available to it to address a very real concern.

One potential method of legitimisation, although not unproblematic given the employment context, is consent.

4. INFORMATION OBLIGATIONS

4.1 Who

For data to be fairly processed, data controllers are obliged, in so far as it is practicable, to provide the data subject with certain information.

4.2 What

This includes:

- the identity of the data controller;
- the identity of a nominated representative of the data controller, if applicable;
- the purpose(s) for which the data are intended to be processed; and
- any other information which is necessary to enable processing in respect of the data to be fair to the data subject.

4.3 Exceptions

The information must only be provided 'in so far as it is practicable'. This is a broad qualification to the obligation.

Please also refer to section 1.3.4 for the general exceptions to the DPA.

4.4 When

The information specified above in section 4.2 must be provided to the data subject not later than the time when the data controller first processes the data. If data are to be disclosed to a third party, then the information must be provided no later than the time of such disclosure.

4.5 How

The data controller is responsible for ensuring the information is 'provided'

or is made 'readily available' to the data subject. There is no further explanation as to how the required information is to be imparted. However this requirement is tempered by the fact that the data controller is only required do this in 'so far as it is practicable'. This substantially dilutes the requirement and provides the data controller with a possible defence to the format in which his information is provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Sections 3 and 4 of the DPA provide a right to the data subject, on written request, to be informed of and be provided the detail as to any personal data being processed.

5.1.2 Exceptions

A general exemption to the right of access under section 4(9) of the DPA provides the right to be supplied with a copy of the information concerned save where 'the supply of such a copy is not possible or would involve disproportionate effect'.

In addition, the right of access to personal data does not apply to personal data listed in section 5 of the DPA, which include data:

(a) kept for the purpose of preventing offences, prosecuting offenders or assessing any tax or other moneys owed or payable to the state;
(b) to which, the right of access does not apply under paragraph (a), and which are kept for the purpose of discharging a function conferred by or under any enactment;
(c) which would be likely to prejudice the security or good order in:
    (i) a prison;
    (ii) a place of detention (as defined in Irish law);
    (iii) a military prison or detention barrack (as defined in Irish law); or
    (iv) Saint Patrick's Institution;
(d) for the purpose of performing functions conferred by any enactment made by the Minister for Justice designed to protect the public against financial loss occasioned by:
    (i) dishonesty, incompetence or malpractice on the part of persons concerned in the provision of banking, insurance, investment or other financial services or similar organisations; or
    (ii) the conduct of persons adjudicated bankrupt;
(e) in respect of which the application of the DPA would be contrary to the interests of protecting the international relations of the state;
(f) kept for the purpose of estimating the amount of the liability of the data controller concerned on foot of a claim for the payment of a sum of money, where this would be likely to prejudice the interests of the data controller;
(g) in respect of which a claim of legal professional privilege could be maintained in court proceedings;
(gg) kept by the DPC or the Information Commissioner (which is a separate

regulator and is responsible for the review of decisions made by certain public bodies on requests for information by members of the public) for the purposes of his or her functions;

(h) kept only for the purpose of preparing statistics or carrying out research where the results of the research are not made available in a form that identifies any of the data subjects; or

(i) that are back-up data.

5.1.3 Deadline

An access request must be complied with as soon as possible and in any event not more than 40 days after compliance with the applicable provisions of the section.

In the case of an access request for results of an examination, the data controller is obliged to comply within 60 days of when the request is made.

5.1.4 Charges

S.I. No. 347/1988 (Data Protection (Fees) Regulations) 1988 provides that an access fee of a maximum €6.35 applies. Often, this is not charged at all by some data controllers as the administration costs of collecting it can be prohibitive relative to the gain.

5.2 Rectification

5.2.1 Right

Data subjects have the right to correct details of their personal data. The data subject must submit a request in writing to the data controller to trigger this right.

5.2.2 Exceptions

There are no explicit exceptions to the right to rectification.

5.2.3 Deadline

The data controller must comply with the request as soon as possible and in any event not more than 40 days after the request was sent. The data controller must then notify the data subject and any person to whom such data were disclosed in the 12 months prior to the request submission of the rectification.

5.2.4 Charges

The access fee stipulated at section 5.1.4 would have to be paid to gain access to the relevant information in the first instance.

5.3 Erasure

5.3.1 Right

Data subjects have the right to erase any of their personal data. There must have been a breach by the data controller of section 2(1) of the DPA (see section 3.4 above) in order for the data subject to benefit from this right.

5.3.2 Exceptions
There are no explicit exceptions to the right to rectification.

5.3.3 Deadline
The data controller must comply with the request as soon as possible and in any event not more than 40 days after the request was sent. The data controller must then notify the data subject and any person to whom such data were disclosed in the 12 months prior to the request submission of the erasure.

5.3.4 Charges
The access fee stipulated in section 5.1.4 would have to be paid to gain access to the relevant information in the first instance.

5.4 Blocking
5.4.1 Right
Data subjects have the right to block any of their personal data. There must have been a breach by the data controller of section 2(1) of the DPA (see section 3.4 above) in order for the data subject to benefit from this right. 'Blocking' is defined in the DPA as marking the data so that it is not possible to process them for the purposes in relation to which they are marked.

5.4.2 Exceptions
There are no explicit exceptions to the right to rectification.

5.4.3 Deadline
The data controller must comply with the request as soon as possible and in any event not more than 40 days after the request was sent. The data controller must then notify the data subject and any person to whom such data were disclosed in the 12 months prior to the request submission of the blocking.

5.4.4 Charges
The access fee stipulated in section 5.1.4 would have to be paid to gain access to the relevant information in the first instance.

5.5 Objection
5.5.1 Right
Data subjects have the right to object, by notice in writing, to the processing or to the commencement of the processing of their personal data where such processing would be likely to cause substantial damage or distress that is unwarranted. The right of objection only applies to processing that is necessary:

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- for the purposes of the legitimate interest pursued by the data controller to whom the data are disclosed, unless those interests are overridden by

the interests of the data subject in relation to fundamental rights and freedoms, in particular the right to privacy.

5.5.2 Exceptions

The right of objection will not apply in a case where the data subject has given his or her explicit consent to the processing, or if the processing is necessary:

- for the performance of, or in order to enter into, a contract to which the data subject is a party;
- for compliance with any legal obligation to which the data controller or data subject is subject other than one imposed by contract; or
- to protect the vital interests of the data subject.

Furthermore the right will not apply to processing carried out by political parties or candidates/holders of elective political office, in the course of electoral activities. The Minister for Justice may also specify further exceptions through regulations, although at the time of writing, he has not yet done so.

5.5.3 Deadline

The data controller must respond with the notice as soon as practicable and in any event not more than 20 days after receipt of the notice. The data subject can apply to the DPC who can in turn serve the data controller with an enforcement notice, if, within 40 days of receipt of the notice, the data controller has failed to reply.

5.5.4 Charges

There are no specific charges in this respect.

5.6 Automated individual decisions

5.6.1 Right

Data subjects have the rights in relation to the automatic processing of their personal data by virtue of section 6B of the DPA. This provides that a decision which either produces legal effects or otherwise significantly affects a data subject may not be based solely on processing by automatic means where the aim of the processing is to evaluate personal matters relating to the data subject. Examples such as work performance, creditworthiness reliability or conduct are given. Moreover, the data subject has a right to be informed free of charge of the logic involved in the processing.

5.6.2 Exceptions

Section 6B provides that the right will not apply where such processing is taken:

- for the purpose of considering whether to enter a contract with the data subject;
- with a view to entering into such a contract; or
- in the course of performing such a contract.

The right also does not apply where the processing is authorised or

required by any enactment and the data subject has been informed of the proposed decision.

However, for any of the above exceptions to apply, it must be established either that: (i) the effect of the decision is to grant a request of the data subject; or (ii) that adequate steps have been taken to safeguard the legitimate interests of the data subject.

5.6.3 Deadline

There is no deadline specified in the DPA.

5.6.4 Charges

There is no charge specified in the DPA.

5.7 Other rights

Not applicable.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

Section 16 of the DPA and the Data Protection Act 1988 (section 16(1)) Regulations, 2007 (the 'Section 16 Regulations') list categories of persons that have to register with the DPC. Registration is compulsory for certain prescribed categories of data controllers and data processors under Regulation 4 of the Section 16 Regulations, which include, in broad terms:

- financial institutions;
- credit institutions;
- insurance undertakings;
- persons engaged in direct marketing/credit reference agencies or debt collectors;
- internet access providers;
- electronic communications networks or service providers;
- persons who process genetic data; and
- data processors that process personal data on behalf of a data controller, in any of the categories listed above.

Regulation 3 of the 2007 Regulations also insinuates that a health professional who processes personal data relating to mental or physical health or the condition of a data subject for medical purposes may be required to register. Even if a data processor/controller does not come within the above mandatory registration requirements, if it cannot show that it falls within the exemptions listed below at section 6.1.3, it will still be obliged to register.

6.1.2 What

The processing of personal data must be notified, unless such processing can benefit from one of the specified exceptions outlined below.

6.1.3 Exceptions

Section 16 of the DPA and Regulation 3 of the Section 16 Regulations set

out certain categories of data processors and data controllers excluded from the registration requirement. In general terms, these categories include data controllers who:

- are not-for-profit organisations;
- only process 'manual data';
- are elected representatives or candidates for electoral office;
- only process data in relation to past, existing or prospective employees in the ordinary course of personnel administration;
- process personal data relating to their past, existing or prospective customers, suppliers, shareholders, directors or officers in the ordinary course of their business;
- process personal data with a view to publishing journalistic, literary or artistic material.

It also includes:

- data processors that only process personal data on behalf of data controllers falling under one of the above exceptions; and
- solicitors and barristers who are data controllers and process data for the purpose of providing professional legal services.

The exemption is limited to the data which are processed squarely within the scope of the exemption.

6.1.4 When

Applications for registration can either be made in writing or online on the Commissioner's website. Registrations last for a period of one year and, at the end of the year, the entry must be renewed or removed from the register.

6.1.5 How

A prescribed application form for registration was set out in Statutory Instrument 351 of 1988. The particulars to be included in the form are:

- name and address;
- purpose or purposes for which the data controller/processor keeps or uses personal data;
- a description of the data;
- persons or categories of persons (other than persons to whom data are disclosed pursuant to section 8 of the DPA, which provides that the restrictions on the processing of personal data under the DPA do not apply in respect of certain persons, such as the certain members of the Irish police force – see section 1.3.4) to whom the data may be disclosed;
- countries or territories to which the data may be directly or indirectly transferred;
- if the source from which the data, and any information intended for inclusion in the data, are obtained is required by the Commissioner to be described in the entry, the persons or categories of persons from whom the data and information are obtained;
- if the data controller is not the person to whom requests for information under section 4 (1) (a) of the Act should be addressed, the name or job status and address of that person;

- the date on which the entry was made or, as the case may be, from which the relevant registration was continued;
- a reference to any other entry in the register relating to the data controller (see section 6.4 below).

6.1.6 Notification fees

The Regulations in S.I. No. 658/2007 (secondary legislation) issued provide that the prescribed fees for a registration application are as follows:

- for applicants with 26 employees or more: €480 (postal application) or €430 (electronic application);
- for applicants with 6 to 25 employees: €100 (postal application) or €90 (electronic application);
- for applicants with 0 to 5 employees or more: €40 (postal application) or €35 (electronic application).

The fee must be enclosed with the registration application. It may be submitted either online via the website of the DPC or by post.

6.2 Authorisation requirements

The DPC does not approve data transfer agreements in Ireland. There is a possibility for the DPC to be the lead data protection commissioner where BCRs are proposed, however this has only occurred in a very small number of cases in Ireland.

6.3 Other registration requirements

None.

6.4 Register

The DPC holds a public register in relation to registrations under section 16 of the DPA (as described above). At the time of writing it was last updated on the 26 September 2011 and is accessible at the following link free of charge: *www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/default.asp&CatID=27&m=g*

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

This is not provided for in Irish legislation. There is an 'authorised officer' who assists the DPC in carrying out his duties, but not one which forms part of a private organisation.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The applicable rules depend on the location of the recipient of the data. If the recipient is within the EEA, there are no limitations on the transfer of personal data.

Transfers are, however, limited depending on whether the personal data are going to a country outside the EEA. In such cases, the country (or territory) must ensure that an 'adequate level of protection' for the privacy

and the fundamental rights and freedoms of data subjects is in place. The adequacy (or otherwise) of the protection must be assessed 'having regard to all the circumstances surrounding the transfer', in particular:

- the nature of the data;
- the purpose and duration of processing;
- the country of origin and of final destination of the data;
- the rules of law in the country of final destination; and
- the relevant codes of conduct and security measures in that country.

8.2 Legal basis for international data transfers

Personal data may be transferred to countries outside the EEA if one of the following conditions is met:

- the transfer of personal data is required or authorised by law;
- the data subject has freely given his or her unambiguous consent to the transfer;
- the transfer is necessary for the performance of a contract to which the data subject is party;
- the transfer is necessary to conclude a contract where the contract is entered into at the request of or in the interests of the data subject;
- the transfer is necessary for reasons of substantial public interest;
- the transfer is necessary for obtaining legal advice or for legal proceedings;
- the transfer is necessary to prevent injury or other damage to the data subject's health or property where it is not possible to inform the data subject;
- the personal data to be transferred are an extract from a statutory public register;
- the transfer is made on the basis of a data transfer agreements; or
- the transfer is made on the basis of binding corporate rules.

8.2.1 Data transfer agreements

A standard set of contractual clauses has been approved by the European Commission to assist companies in complying with the obligation to ensure 'adequate protection' for personal data transferred outside the EEA. These can be used without seeking the DPC's authorisation. The DPC, however, does have the power to endorse 'model contracts' in specific circumstances, as well as the power to approve particular contracts that provide satisfactory safeguards.

In practice however DPC-approved data transfer agreements are not used frequently in Ireland.

8.2.2 Binding corporate rules

A company may also comply with its data protection requirements through the adoption of binding corporate rules. These are binding internal codes of conduct requiring that the company and its employees comply with data protection norms. Ireland does mutually recognise the BCRs and the DPC can be the lead data protection authority in a BCR process. However, these are not frequently commenced in Ireland.

8.2.3 Safe Harbour

In the absence of coming within the above listed exceptions, data transfers from the EEA to the US may take place only where the US company receiving the data has signed up to the 'Safe Harbour' scheme. DPC authorisation is not required.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

There are no provisions relating specifically to the confidentiality of data in Irish legislation implementing the Directive. Section 21(1) of the DPA does provide, in relation to data processors, that personal data cannot be disclosed by him, or an agent/employee of his, without the prior authority of the data controller on behalf of the data subject.

9.2 Security requirements

Both data controllers and data processors have obligations to ensure the security of personal data in their control. They must ensure that there are security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of data and against all other unlawful forms of processing. The respective obligations of the data processor and data controller are detailed further in section 2C of the DPA.

In determining the appropriate security measures to be provided, several factors are laid down in the DPA to which a data controller may have regard. These include the state of technological development and the cost of implementing the measures. While these factors are phrased in a facultative manner, nonetheless, whatever measures adopted should ensure that the measures are appropriate to the potential harm that might result from unlawful processing and the nature of the data concerned.

A data controller has further obligations where personal data are being processed to ensure:

- a written contract is in place providing that processing takes place on specific instructions from the data controller;
- the data processor provides sufficient guarantees in respect of the technical security measures, and organisational measures governing the processing.

Finally, the Personal Data Security Breach Code of Practice was published on 29 July 2011 by the DPC. This is discussed further in the next section.

9.3 Data security breach notification obligation

There is no specific statutory obligation to notify a breach under the DPA, however, the DPC recently issued the Data Security Breach Code of Practice (the Code) which governs this area in Ireland. This Code does not yet have the force of law. The DPA provides that it could have force of law if presented before the Irish Parliament, but this has not occurred as yet. The Code does not apply to providers of publicly available communications networks or services, which are governed by the 2011 Regulations.

9.3.1 Who

Under the Code, the data controller is responsible for making the notification.

9.3.2 What

The Code provides that the DPC is entitled to request a data controller to provide a detailed written report of the incident. This should include the following elements:

- the amount and nature of the personal data that have been compromised;
- the action being taken to secure and/or recover the personal data that have been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.

9.3.3 To whom

The Code states that where there is risk of unauthorised disclosure as a result of the breach, the data controller must give 'immediate consideration' to informing the data subject and any other relevant authority (eg, the police force in Ireland) including the DPC himself. The DPC does not have to be informed if:

- the data subjects have been notified;
- the breach affects no more than 100 data subjects; and
- the breach does not involve information of a sensitive or financial nature.

9.3.4 When

Under the Code, the DPC will specify a timeframe for the delivery of the report based on the nature of the incident and the information required.

9.3.5 How

The Code does not prescribe a format for the breach notification. The content is specified above in section 9.3.4.

9.3.6 Sanctions for non-compliance

Under the 2011 Regulations, the DPC can prosecute companies for failure to take appropriate security measures or failing to report data security breaches, with fines of up to €250,000. Failure to notify the data subject can lead to fines of up to €5,000 per breach.

9.4 Data protection impact assessments and audits

The DPC may carry out any investigations necessary to ensure compliance

with the provisions of the DPA. However, there is no provision in the DPA regarding data protection impact assessments and audits carried out by private organisations.

9.4.1 Who

The DPC conducts the audits.

9.4.2 What

The audits usually take the form of investigations of selected entities. The DPC seeks to identify any areas of concern regarding the nature or manner in which the entity handles personal data.

9.4.3 When

A number of audits are conducted throughout the year. For example, in 2009, the DPC undertook a data protection audit of the Irish Revenue.

9.4.4 How

An entity is given advanced notice of the audit and is asked to provide a report on its data protection practices. A team of investigators sent from the DPC will usually inspect the premises of the entity. A report, including recommendations, is then prepared. While the entity is not legally obliged to comply with the report, the DPC may follow up at a later date to evaluate how the recommendations have been acted on. Breaches of data protection law discovered on the basis of this may be pursued in the normal way, as outlined in the next section.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The DPC may investigate a complaint of breach of the DPA and seek to arrange an amicable resolution of the complaint.

If a resolution is not achieved, the DPC may, if he considers that the data controller or data processor is in breach of the DPA, issue a written notice, termed an 'enforcement notice'. This may prescribe steps (detailed above in section 5), including correcting/blocking/destroying or erasing the data concerned.

Failure to comply with an enforcement notice (without reasonable excuse) constitutes an offence under the DPA. Enforcement notices may be challenged before the court; however, it seems that courts may be reluctant to overturn the DPC's view on a matter given his special role under the DPA.

10.2 Sanctions

In addition to the regulatory sanctions outlined above, the Irish courts also have a general jurisdiction to order rectification, blocking or erasure of personal data if deemed appropriate.

Where an offence is committed under the DPA, whether for breach of an enforcement notice or a specific offence provided for by the Acts, the maximum penalty is a fine not exceeding €3,000 for a summary conviction

(ie, before a judge in the District Court) or €100,000 for a conviction on indictment (ie, before a judge and jury in the Circuit Court). A breach of data protection law is not punishable by imprisonment.

Where an offence under the DPA occurs with the consent or as a result of the negligence of a director, manager, secretary or other officer of the company, that individual may be personally liable, and criminal proceedings may be brought against him or her.

With regard to civil remedies, the DPA imposes a duty of care on data controllers and data processors with respect to any data subjects whose personal data they process. Therefore, in the event of a breach of the DPA by a data processor or data controller a data subject may be able to bring an ordinary suit in negligence for breach of this duty of care. We are unaware of any case in which such a claim has been brought.

Along with formal enforcement actions, the DPC operates a 'name and shame' policy. The DPC often releases the names of data controllers and data processors under investigation and against whom orders have been made in case studies and annual reports as well as, in certain limited cases, in press releases.

10.3 Examples of recent enforcement of data protection rules

The DPC has the power to serve Enforcement Notices or Information Notices as provided for in the DPA. In 2010, Enforcement Notices were served on six companies including Bus Éireann (a public transport provider) for failure to provide access to individuals' information under section 4(1) of the DPA. The majority of Enforcement Notices were issued as a result of breaches of this section of the DPA. Information Notices were issued to seven companies during the same period.

In 2010, the DPC successfully prosecuted several companies including Tesco. The DPC had received several complaints from individuals who had attempted to unsubscribe from receiving marketing emails from Tesco, but had continued to receive such emails. Tesco was successfully prosecuted in Dublin District Court. The Court imposed penalties of €1,000 in respect of each charge and ordered that Tesco pay the DPC's legal costs.

In 2009, Home RBVR, trading as Brasserie Sixty6 (a restaurant), was among the companies prosecuted by the DPC. The company had repeatedly sent marketing text messages without the recipients' prior consent. The company was convicted of four offences and fined a total of €3,250 in Dublin District Court.

10.4 Judicial remedies

If there is a breach of the DPA as a result of negligence of a director, manager, secretary or other officer of the company, criminal proceedings may be brought against that person.

10.5 Class actions

These do not exist in Ireland.

10.6 Liability

Section 7 of the DPA implies a duty of care in the relationship between data controller/processor and the data subject. This facilitates an action in negligence for breach of this duty of care which could, foreseeably, include an action in damages. This is not common and we are unaware of any examples of recent case law in this respect. In any event, a data subject would still be under a duty to mitigate his/her losses even if negligence was proven.

Romania

Nestor Nestor Diculescu Kingston Petersen
Roxana Ionescu & Ovidiu Balaceanu

1. LEGISLATION

1.1 Name/title of the law

In Romania the right to privacy is generally regulated by various legal enactments, the most important of which is the Romanian Constitution (which mentions the right to privacy in Article 26 'Intimate, Family and Private Life' of Chapter II 'Fundamental Rights and Freedoms').

The processing of personal data is mainly regulated by Law No. 677 of 21 November 2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as subsequently amended (the Data Protection Law or DPL). This enactment transposes into Romanian law the Data Protection Directive 95/46/EC (the Directive), and is generally in line with it. Particular rules (eg, exemptions to notification obligations, rules on the transfer of personal data abroad, minimum security standards for processing operations) are further provided in secondary legislation enacted by the Romanian Ombudsman (as the former data protection authority) and, from 2005, by the National Authority for the Supervision of Personal Data Processing (the DPA).

In the electronic communications sector, Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, as subsequently amended (the e-Privacy Law), also applies. The e-Privacy Law transposes the ePrivacy Directive 2002/58/EC, although the latest amendments to this directive have yet to be fully transposed in Romania.

1.2 Pending legislation

On 14 June 2011 a proposal amending and unifying Romanian telecom legislation (Pl-x nr. 393/2011) was submitted to the Romanian Parliament. However, due to the lengthy law-making procedure in the Romanian Parliament and the imminence of infringement proceedings due to the failure to transpose on time EU Directives 2009/140/EC and 2009/136/ EC, the Government of Romania chose to implement the new legislation in the emergency procedure through a Government Emergency Ordinance and on 20 October 2011 published on the website of the Ministry of Communications and Information Society, for public consultation, the draft Government Emergency Ordinance on electronic communications (the Draft Telecom Law). Among others, the Draft Telecom Law transposes into Romanian law parts of the Directive 2009/136/EC which amends, among others, the e-Privacy Directive. In connection with personal data

protection, the Draft Telecom Law sets forth new obligations in connection with the security and integrity of public communications networks and publicly available electronic communications services through public communications networks, including in case of breaches or losses in relation thereto (see section 9.3 below).

On 23 June 2011, the Romanian Ministry of Communications and Information Society posted on its website for public consultation, a proposal for the transposition into Romanian law of the Data Retention Directive 2006/24/EC. However, according to the information recently published on the website of the DPA, the authority has not endorsed the proposal. On 27 October 2011, the European Commission started infringement procedures against Romania for failure to transpose the Directive, formally requesting Romania through a reasoned opinion to ensure transposition of the Data Retention Directive within two months.

On 7 October 2011, the Romanian Ministry of Communications and Information Society made available for public debate a proposal for the amendment of the e-Privacy Law for the transposition of the provisions of Directive 2009/136/EC, which amends the e-Privacy Directive. The draft legislation ensures the transposition of Directive 2009/136/EC. Furthermore, the draft legislation introduces additional provisions, most notably regarding:

(i) clarifying the scope of application of the e-Privacy Law;
(ii) enhancing the competences of the DPA in the field of the processing of personal data in the electronic communications sector (including by expressly offering it the right to audit the security measures taken by the provider of publicly available electronic communication services and the provider of public communication networks);
(iii) introducing an opt-out rule for the establishment of directories of subscribers; and
(iv) regulating a specific method for obtaining consent for the storage of traffic data by the provider of a publicly available electronic communications service, eg, in the context of cookies (see section 3.3 below).

In addition, the DPA posted on its website draft normative decisions on: (i) approving minimum security requirements in respect of personal data processing (see section 9.2 below); (ii) the conditions on which the personal numeric code and other personal data of general identification may be processed (see section 1.3.2 below); and (iii) on personal data processing and audio/video surveillance (see section 3.6 below).

1.3 Scope of the law

1.3.1 The main players

- The 'data controller' is any natural or legal person, private or public body, including public authorities, institutions and their territorial structures, which establishes the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by or based on a legal enactment, the data controller

is the natural or legal person, private or public body designated as data controller by or based on that legal enactment. Although the DPL generally qualifies data controllers as natural or legal persons (thus excluding entities without legal personality such as branches or representative offices), in practice the DPA deems that in some cases, branches or representative offices of foreign legal persons may also be deemed data controllers for the purposes of the processing operations carried out in Romania and, hence, they also have to comply with the requirements set by such laws.

- The 'data processor' is any natural or legal person, private or public body, including public authorities, institutions and their territorial structures, which processes personal data on behalf of the data controller (except for the persons who, under the direct authority of the data controller or the data processor, are authorised to process the data).
- The 'data subject' is an identified or identifiable natural person, the latter being an individual who can be directly or indirectly identified, 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.
- The 'third party' is any natural or legal person, private or public body, including public authorities, institutions and their territorial structures, other than the data subject, the data controller, the data processor or the persons who, under the direct authority of the data controller or the data processor, are authorised to process data.

1.3.2 Types of data

Romanian privacy laws generally apply to data regarding natural persons but not legal persons (eg, companies). By exception, the e-Privacy Law extends the protections set out for the processing of personal data in connection with the sending of unsolicited commercial communications to legal persons as well.

'Personal data' are defined as 'any information relating to an identified or identifiable natural person, ie, the data subject', and may include various information such as an individual's name, address, image, voice, telephone number, bank account number, etc.

The DPL explicitly mentions certain categories of sensitive data which are generally subject to stricter processing conditions:

(i) special categories of personal data, ie, 'personal data regarding racial or ethnic origin, political, religious or philosophical or other similar convictions, trade union membership, as well as personal data concerning health condition or sex life';
(ii) personal data of general identification, eg, 'personal numeric code'.
(iii) personal data regarding criminal offences or contraventions, ie, 'personal data regarding the perpetration of criminal offences by the data subject, or criminal convictions, safety measures or administrative or contravening sanctions applied to the data subject'.

Although not explicitly provided in the DPL, under the secondary

legislation enacted for its application, other data such as the series and number of identity documents, genetic data and biometrical data, are also deemed sensitive data, and are consequently subject to the stricter processing conditions applicable to such data.

Personal data that have become anonymous (ie, data that, according to the DPL, due to its origins or the specific manner of processing, may no longer be associated with an identified or identifiable person, which needs to be assessed on a case-by-case basis) are no longer subject to the rules of Romanian privacy laws (as long as they meet the anonymity requirements).

1.3.3 Types of acts/operations

The DPL applies to 'processing' of personal data, which is defined as 'any operation or set of operations which is performed upon personal data, by automatic means, as well as otherwise than by automatic means if the personal data processed are included or are intended to be included in a filing system such as: the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure to third persons by means of transmission, dissemination or other means, alignment or combination, blocking, erasure or destruction'.

A 'personal data filing system' is defined as any organised structure of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed according to functional or geographical criteria. Accordingly, in relation to non-automated processing of personal data, the DPL applies provided that such processing is structured as described above.

The secondary legislation enacted for the application of certain provisions of the DPL specifies certain personal data processing operations which are deemed to pose specific risks to individual's rights and freedoms by virtue of the nature of the data processed, the processing purposes, the specific categories of data subjects, or the means used for the processing (such operations include, among others, processing operations in respect of sensitive data). These processing operations are generally subject to prior control and authorisation by the DPA (see also section 6.2 below).

1.3.4 Exceptions

The processing of personal data by natural persons exclusively for their personal use, provided that such data are not intended to be disclosed, falls outside the scope of application of the DPL. In addition, the DPL does not apply to personal data processing and transfers made within the framework of the activities performed in the fields of national defence and national security within the limits and restrictions set out by law.

Moreover, partial exemptions from the rules set out by the DPL are provided in relation to personal data processing done for certain purposes (including statistic, journalistic, artistic, literary, historical or scientific research, or purposes), as well as to the personal data processing and transfers abroad made within the context of the activities of prevention, investigation and fighting of criminal offences and maintenance of public

order, and other activities performed in the field of criminal law.

1.3.5 Geographical scope of application

Romanian data privacy laws apply to personal data processing operations carried out within the context of the activities performed by:

- data controllers established in Romania;
- Romania's diplomatic missions or consulate offices; and
- data controllers not established in Romania, to the extent that the data are processed by any means located in Romania and such means are used for more than transit purposes. In respect of such processing, the foreign data controllers must designate persons established in Romania as their representatives. The provisions of the DPL shall also apply to the representatives of foreign data controllers, however, without prejudice to the possibility that legal actions can be initiated directly against the foreign controllers.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

National Supervisory Authority for Personal Data Processing (*Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal*)
28-30 Magheru Boulevard, 1st District, Bucharest, Romania
T: +40-21-252.58.88
F: +40-21-252.57.57
E: anspdcp@dataprotection.ro
W: *www.dataprotection.ro*

From 1 November 2011 the DPA will change headquarters to the address indicated above, but it has not yet provided the new telephone and fax contact details.

The DPA is run by a president and a vice-president who are appointed by the Romanian Senate. In exercising his attributions, the president of the DPA issues decisions and guidelines having normative character, which are binding, in relation to the processing of personal data, on all the institutions and entities. In addition, the president submits to the Romanian Senate annual reports regarding the authority's activities.

The DPA's organisational structure is also subject to endorsement by the Romanian Senate.

2.1 Role and tasks

The DPA is an independent, autonomous and impartial public authority and its primary objective is to ensure that individuals' fundamental rights and liberties, and in particular their right to privacy, are protected in connection with personal data processing and the free movement of such data.

The authority must be consulted when legal proposals regarding the protection of rights and liberties in relation to the processing of personal data are drafted, and may propose the initiation of new proposals or the

amendment of legislation currently in force in fields relating to personal data processing. It also cooperates with public authorities and bodies of public administration; centralises and analyses such authorities/bodies' annual activity reports regarding the protection of personal data; and makes recommendations and issues endorsements on any matter relating to personal data processing, upon the request of any person, including the public authorities and bodies of public administration.

The authority also monitors and controls the lawfulness of personal data processing and imposes sanctions if it ascertains breaches of the applicable rules (see also section 10 below).

2.2 Powers

The DPA has the following main powers:

- to issue templates for notification forms and registers;
- to receive and review personal data notifications, and to communicate to the data controllers the results of such review and of controls performed by it in connection to them;
- to authorise personal data processing and data transfers when such authorisation is required by law;
- to inspect personal data processing on its own initiative or based on complaints and to impose sanctions for breaches of the data protection rules set forth by law;
- to provide information to the individuals and/or legal entities performing activities in data protection related fields, on the need to observe the obligations and procedures provided by the data privacy laws;
- to keep and make available to the public the register where notified personal data processing notifications are recorded;
- to cooperate with similar foreign authorities for the purposes of providing mutual assistance, as well as with persons established abroad, for the purposes of defending fundamental rights and liberties which may be affected through the processing of personal data;
- to issue recommendations and endorsements on any matter relating to the protection of fundamental rights and liberties concerning personal data processing.

(See also section 2.1 above).

2.3 Priorities

Every year, the DPA prepares and publishes on its website, a report regarding its activities during the preceding year (including its priorities in that year).

The 2009 activity report mentioned as priorities: (i) preparedness in order to support the Schengen Evaluation Mission with respect to personal data processing in view of Romania's accession to the Schengen area; and (ii) addressing complaints filed to the authority by individuals. No information on 2010 and 2011 priorities have been made public by the DPA to date.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Under the Romanian data privacy laws, the data subject's consent may constitute one of the possible legal bases for the processing (including transfers abroad) of both non-sensitive and sensitive personal data.

In respect of processing of anonymous data, the DPL provides as a general rule that the data subject's consent is not required for the processing of regular anonymous personal data (ie, non-sensitive personal data) for statistical and scientific reasons, provided the data's anonymity is maintained for the entire duration of the processing. Arguably, consent for the processing of sensitive data is still necessary as long as there is a possibility for such data to lose their anonymity during the processing operations.

The DPL does not provide a specific definition of consent in the field of personal data protection. Romanian data privacy laws only require that such consent be given in an explicit, unequivocal manner, and sometimes in writing (see section 3.1.2 below).

3.1.2 Form

The DPL requires that consent for the processing be given in an explicit and unequivocal manner.

However, in certain cases such consent is not deemed valid unless it is obtained in a specific form. For example, for processing personal data regarding health (other than by or under the supervision of a health professional), or in the case of transfers of sensitive data relying only on the data subjects' consent to countries which are not deemed to provide an adequate level of protection, the data subjects' consent must be given in writing.

3.1.3 In an employment relationship

There are no specific rules regarding consent in the employment relationship. In practice, to date the DPA has not raised objections in respect of employers basing their personal data processing operations on (potential) employees' consent, provided that the processing complies with the general personal data rules provided by the Romanian data privacy laws. In fact, it is more likely that the DPA would object to processing operations involving the personal data of employees on the grounds that they are in breach of adequacy or non-excessiveness requirements set under the law, rather than object to the legitimacy of the processing that relies on the data subjects' consent.

3.2 Other legal grounds for data processing

In the absence of a data subject's explicit and unequivocal consent, non-sensitive personal data may be processed if one or more of the following conditions are met (however, without prejudice to the legal provisions regarding a public authority's obligations to respect and protect intimate, family and private life). The processing is necessary:

- for the performance of a contract or pre-contract to which the data subject is party, or in order to take certain measures at the request of the data subject before entering into a contract or pre-contract;

- to protect the life, physical integrity or health of the data subject or of another person in danger;
- for compliance with a data controller's legal obligation;
- for the performance of certain measures of public interest, or which envisage the exercise of official authority prerogatives vested in the data controller or in a third party to whom the data are disclosed; or
- for the purposes of achieving a legitimate interest pursued by the data controller or by the third party to whom the data are disclosed, provided that such interest does not harm the interests or fundamental rights and freedoms of the data subject; or
- regarding data obtained from documents accessible to the public according to the law; or
- when done exclusively for statistical, historic or scientific research, and the data remain anonymous throughout the entire duration of the processing.

As a general rule, processing the sensitive data mentioned in section 1.3.2 above is prohibited, unless certain exemptions/conditions explicitly provided by law apply. Such data may be processed if the data subject has given his explicit consent (provided that this consent can be withdrawn by the data subject at any time), or if the processing, without prejudice to the legal provisions regarding a public authority's obligations to respect and protect intimate, family and private life:

- is necessary for the data controller to comply with its specific labour law obligations or rights (however provided that the warranties provided by law are observed);
- is necessary to protect the life, physical integrity or health of the data subject or of another person, where the data subject is physically or legally incapable of giving his consent;
- is done, within its legitimate activities, by a foundation, association or any other political, philosophical, religious or trade union organisation with non-lucrative purpose, provided that the data subject is a member of such organisation or has with it regular relations concerning the specifics of such organisation and the data are not disclosed to third parties without the data subjects' consent;
- relates to personal data which have been manifestly made public by the data subject;
- is necessary for the establishment, exercise or defence of a right before the courts of law;
- is necessary for purposes of performing some health sector specific activities, such as preventive medicine, provided that the processing is done by or under the supervision of a health professional bound by professional secrecy or by or under the supervision of another person bound by an equivalent secrecy obligation; or
- is explicitly required by law for protection of an important public interest (provided that the processing is done by observing the data subject's rights and other warranties provided by law); or
- (in case of personal data regarding the condition of someone's health)

is necessary for the protection of public health or for the prevention of an imminent danger, of the perpetration of a criminal deed or the occurrence of such deed's result, or for the elimination of such deed's adverse effects.

The personal data of general identification mentioned in section 1.3.2 (ii) above may be processed if the data subject has given his explicit consent or if the processing is explicitly provided by a legal provision.

The personal data regarding criminal offences or contraventions mentioned in section 1.3.2 (iii) above may be processed only by or under the control of the public authorities, within the limits of their legal competencies and the conditions set out in the special laws applying in these fields. A complete register of criminal convictions may be kept only under the control of competent public authorities.

Under the DPL, theoretically the DPA may also establish other cases when these data may be processed, provided adequate safeguards for the observance of the data subjects' rights are established; however, it has not yet done so.

On 5 August 2011, the DPA posted for public consultation a draft normative decision regarding the conditions on which the personal numeric code and other personal data of general identification may be processed. No proposed or expected deadline has been provided for the entering into force of this decision. The draft decision provides, among others, for detailed safeguards to be implemented by data controllers when processing such data with the data subjects' consent (ie, when the processing is not required by law). Such safeguards include: (i) the appointment in writing of the person(s) who will process the data and will be responsible for keeping the confidentiality of such data; (ii) the appointment in writing of a person specialised in information security, who will supervise the data processing, including the proper functioning of the information systems used for the processing; (iii) the establishment of an information security plan mainly including the technical information security and the security of the areas where the processing is carried out.

Part of the restrictions provided by law in respect of the special categories of personal data mentioned in section 1.3.2 (i) above and the personal data regarding criminal offences or contraventions mentioned in section 1.3.2 (iii) above do not apply where the processing is done exclusively for journalistic, literary or artistic purposes, provided that the processing envisages personal data which has been manifestly made public by the data subject or which are closely linked to the data subject's public person status or the public character of the deeds in which the data subject is involved.

3.3 Direct marketing and cookies

The processing of personal data for the purpose of direct marketing is subject to the general personal data protection rules provided by the DPL and certain specific rules provided by the e-Privacy Law and Romanian e-commerce laws.

In terms of particular rules, the e-Privacy Law and the Romanian

e-commerce laws, ie, the Law No. 365 of 7 June 2002 on electronic commerce and the Government Decision No. 1308 of 20 November 2002 approving the Methodological Norms for the application of Law No. 365/2002 on electronic commerce prohibit the sending of unsolicited commercial communications through any method using electronic communication services open to the public (eg, telephone, fax, SMS, email, etc) when the targeted subscriber/addressee has not given his/her prior explicit consent to receive such communications. This prohibition applies both in relation to legal and natural persons. In addition, the laws require that certain specific formalities be observed if it is envisaged that the addressees' prior explicit consent will be obtained through electronic mail for sending commercial communications via email.

The use of cookies or equivalent devices is currently regulated by the e-Privacy Law. Under this law, the use of an electronic communications network for purposes of storing information on a user/subscriber's terminal equipment is generally permitted only if the user/subscriber: (i) has been provided with clear and complete information as required by the DPL, in particular on the purposes of the storage of data; and (ii) has been offered the possibility to refuse the storage of data. As an exception, the storage of data is permitted when: (i) it is done for the exclusive purpose of performing or facilitating the transmission of a communication through an electronic communications network; or (ii) it is strictly necessary for supplying a service from the information society which has been explicitly requested by the user/subscriber.

Romania has not yet transposed into its national law the new requirements concerning the use of cookies introduced by Directive 2009/136/EC. However, the draft legislation for the transposition of Directive 2009/136/EC covers these aspects and provides that the consent for cookies may be granted also through the use of the settings of the internet browser or of other technologies through which it may be considered that the subscriber or the user expressed his agreement, as well as through the listing by the subscriber or user of providers to which the subscriber or user prohibits the storage of information or the access to the information stored.

3.4 Data quality requirements

Pursuant to the DPL, personal data processing operations may only be carried out in good faith, for defined, legitimate purposes, and if the processed data are adequate, pertinent and non-excessive considering the declared purposes of the processing.

The personal data collected for a specific processing purpose may not be later used for other incompatible purposes, without the prior information and consent of the individuals to whom the data belong (when such consent is required by law). Further processing of personal data for statistical and historical or scientific research is not deemed incompatible with the purpose of their collection if certain conditions provided by law are met.

Moreover, the processed personal data must be accurate, kept up to date and stored in a form permitting identification of data subjects, and only

for the duration necessary for the achievement of the processing purposes (as an exception, under certain conditions, it is permitted to store personal data for a longer duration, for statistical and historical or scientific research). Appropriate measures must be taken in order that inaccurate or incomplete data be erased or rectified.

3.5 Outsourcing

When outsourcing data processing activities to data processors, the data controller is required to select data processors who ensure sufficient safeguards in respect of the technical security and organisational measures for the envisaged processing, as required by law, supervise the data processors' compliance with these measures and ensure the data processors' compliance with the personal data processing rules mentioned in section 3.4 above. To achieve this, data controllers are required to enter with the data processor into written agreements which must provide, as a minimum, the data processors' obligations to:

- act only within the limits of the instructions received from the data controllers in connection with the processing carried out on data controllers' behalf; and
- implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, in accordance with the requirements of the applicable data protection laws.

If the data processors are established abroad, in countries which are not deemed to ensure an adequate level of protection for the data subjects' rights, the agreements with the data processors should, as a rule, observe the standard contractual clauses approved by European Commission for the transfer of personal data to processors established abroad.

Although not explicitly provided by Romanian data protection laws, considering the data controllers' responsibility in respect of any personal data processing carried out on their behalf, if the data processor intends to sub-contract part of the data processing, the same obligations vesting with them should be imposed on the sub-processor. Moreover, the subcontracting should be done with the prior information and consent of the data controller. In practice, the DPA is reluctant to accept the appointment of sub-processors, even though such practice was slightly improved by the approval of the European Commission's 2010 standard contractual clauses for controller-to-processor transfers, which contemplate the possibility of using sub-processors.

3.6 Email, internet and video monitoring

3.6.1 General rules

Romanian law does not explicitly prohibit email, internet and video monitoring, but it has to be done in compliance with the general privacy principles, rules and requirements provided by the Romanian Constitution,

the Romanian Criminal Code and the DPL, including in respect of the legitimacy of the monitoring purposes, the requirement that the data be adequate, pertinent, non-excessive and the monitoring be implemented in a transparent manner.

Under the Romanian Criminal Code, unlawful accessing, interception, disclosure of the content of a correspondence, conversation or communication performed by any means of distance transmission qualifies as criminal offence. The Criminal Code does not make any distinction in respect of monitoring in an employment or other context.

The e-Privacy Law also generally prohibits the listening, recording, storage and any other form of intercepting or surveillance of communications transmitted through electronic communication public networks and of related traffic data, as well as the accessing of information stored on a user/subscriber's terminal equipment by using an electronic communications network, with certain exceptions.

As to permitted use of video surveillance cameras, while no explicit legal provisions are currently in force, pursuant to a draft decision on personal data processing through the use of audio/video surveillance recently published for public consultation on the DPA's website (the Draft Audio/Video Surveillance Decision):

- the monitoring is allowed in both public and private areas, by observing the principles of purpose proportionality and legitimacy, and only if other prevention, protection and security measures clearly prove to be insufficient and/or inapplicable;
- the monitoring may be done for a limited number of purposes, including: to prevent and combat the perpetration of criminal offences, to ensure the security of persons and goods, to obtain means of evidence or for other legitimate purposes, provided that such purposes do not harm data subjects' fundamental rights and liberties, or interest;
- real time capturing of images without storage, is not deemed to be personal data processing;
- processing of personal data through video monitoring is prohibited if carried out exclusively in relation to racial or ethnic origin, political or religious convictions, trade union membership and sex life;
- the monitoring is prohibited in areas intended for exclusively private activities such as changing rooms, shower rooms, toilets, etc;
- personal data must be kept for a period proportional to the processing purpose, in any case not exceeding 30 days.

Installing video monitoring cameras generally requires prior: (i) authorisation from the local police; and (ii) notification to the DPA. In some cases it may also require prior special endorsement from the authorities provided under the legislation on protection of classified information.

While no explicit legal provisions are currently in force, the DPA's Notifications Guideline (see section 6.1.2 below) and the Draft Audio/Video Surveillance Decision also provide requirements on:

- how data controllers should ensure that individuals are adequately informed of the processing of their personal data through video

monitoring means; and
- limitations on the viewing of the images which may be processed through the video cameras, depending on the type of area (public or private) subject to monitoring.

3.6.2 Employment relationship

In addition to the general rules mentioned in section 3.6.1 above, email, internet and video monitoring within an employment relationship has to be done in compliance with the rights to privacy and dignity in the workplace, as well as the rights to be informed and consulted in matters concerning the activities performed for the employer, which are recognised by employees under Romanian Constitution and labour legislation.

According to the Draft Audio/Video Surveillance Decision, using video surveillance cameras in the workplace will only be permitted for the purpose of ensuring compliance with explicit legal requirements, by observing employees' rights, including the right to be informed in advance.

4. INFORMATION OBLIGATIONS

The rules provided in this section 4 do not apply in the case of activities performed in the fields of national defence and national security, provided that, by application of these rules, the efficiency of action or the goals pursued within the fulfilment of the public authorities' legal duties are harmed. However, such lack of application is strictly limited to the time necessary for the achievement of the goals pursued by the performance of the above-mentioned activities.

4.1 Who

Data controllers are responsible for informing the data subjects about the processing of personal data relating to them.

4.2 What

As a general rule, the data controller must provide the following information to the data subject:
- the identity of the data controller and of his representative, if any;
- the purpose(s) of the data processing; and
- additional information (depending on whether the personal data are obtained directly from the data subject or not) such as: the recipients or categories of recipients of the processed data; whether the provision of all the requested data is compulsory and the consequences of the refusal to provide them; the existence of the data subject's rights provided by the law and the conditions in which such rights may be exercised; and the categories of processed data.

The data controller is exempted from providing the above information if:
- the data subject is already aware of the information; or
- (when the data are not obtained directly from the data subject) if:
  (i) the data processing is done exclusively for journalistic, literary or artistic purposes and the provision of such information would give

indications on the source of information; or
(ii) when the processing of the data is done for statistic, historic or scientific research; or
(iii) in any other cases when providing this information proves impossible or would require a disproportionate effort compared with the legitimate interest that may be harmed; or
(iv) in cases when recording or disclosure of the data is expressly laid down by law.

4.3 When

When the data are obtained directly from the data subject, the information should be provided before beginning the processing.

When the data are not obtained directly from the data subject, the information should be provided at the time the personal data are collected or at the latest when the data are disclosed for the first time.

4.4 How

The DPL does not explicitly provide the manner in which the information must be provided to the data subjects. The secondary legislation enacted for the application of the DPL ie, Decision No. 95 of 11 December 2008 of the President of the DPA, for the establishment of the template form for the notifications provided by Law No. 677/2001 sets forth the main alternatives for providing the information to data subjects, namely:
(i) in writing;
(ii) by posting on the web page;
(iii) by posting at headquarters; or
(iv) verbally.

The DPA has also issued certain clarifications and recommendations on this matter in the Notifications Guideline (see section 3.6.1 above). According to this guideline, the data subjects' information should be provided in an adequate manner considering the specific circumstances of the processing operations carried out, and, from all methods of information provided in Decision No. 95/2008, the verbal method should be used only exceptionally (ie, whenever the information cannot not be provided by any other methods).

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Data subjects are entitled to obtain from the data controller, upon their written, dated and signed request, confirmation on whether their personal data are processed or not by the data controller. If processing the data subjects' personal data, the data controller must accompany the above-mentioned confirmation with information regarding at least:
(i) the purposes of the processing, the categories of the personal data concerned, the recipients or categories of recipients to whom the data are disclosed; communication, in an intelligible form, of the processed

personal data and any information available to it in respect of these data's origin;
(ii) information regarding the functioning principles of the mechanism through which any automated processing of personal data is done;
(iii) information regarding the existence of the data subjects' right of intervention upon the data and the right to object, and the conditions for exercising these rights; and
(iv) information on the possibility to consult the online Notifications Registry kept by the DPA (see section 6.4 below), to file claims before this authority and to the courts.

In their request for the above-mentioned information, the data subjects may indicate to the data controller a certain address where such information should be communicated to them (which may be an electronic one or a mail service ensuring that the delivery is made personally to them).

When processing health related personal data, the information request and the answer to it may be filed by/communicated to the data subject or a health professional acting on the data subject's behalf.

5.1.2 Exceptions

The same exception as for the information obligations applies (see section 4 above).

The right of access may be refused where the data subjects' personal data are processed exclusively for journalistic, literary or artistic purposes, and the provision of the information mentioned in section 5.1.1 above would lead to information sources being revealed.

5.1.3 Deadline

The data subjects may exercise their right of access at any time. The data controller must provide the information within 15 days as of the date it receives the request. Access to health-related data that are processed for scientific research purposes may generally be delayed if, at least apparently, there is no risk that the data subjects' rights will be harmed and the data are not used for taking decisions or measures towards a certain person, and to the extent that the delay may not affect the proper performance or the results of the research. However, the access may not be provided later than the time the research is finalised.

5.1.4 Charges

The data subjects' entitlement to exercise their right to access is free of charge for one request per year.

5.2 Rectification

5.2.1 Right

Data subjects have the right to obtain from the data controller, by means of written, dated and signed request: (i) the rectification of their personal data processed in breach of the DPL's provisions, particularly incomplete or inaccurate data; and (ii) the notification of third party recipients of the data

in respect of such rectification, provided that the notification does not prove to be impossible or does not entail a disproportionate effort compared to the legitimate interest which may be harmed in the absence of notification.

In their data rectification request, the data subjects may indicate to the data controller a certain address where the data controller may communicate to them the measures taken in order to address their request.

5.2.2 Exceptions

The same exception as for the information obligations applies (see section 4 above).

5.2.3 Deadline

The data subjects may exercise their right to rectification at any time.

The data controller must communicate to the data subjects the measures taken in respect of the rectification and notification, as well as the name/s of the third party/ies to which the personal data subject to rectification have been disclosed (if the case may be), within 15 days of the date it receives the rectification request, and in the manner indicated by the data subjects.

5.2.4 Charges

The data subjects' entitlement to exercise their right to rectification is free of charge.

5.3 Erasure

See section 5.2

5.4 Blocking

See section 5.2

5.5 Objection

5.5.1 Right

Data subjects have the right to object to the processing of their personal data based on justified and legitimate reasons relating to their particular situation. The personal data in respect of which the data subjects have made legitimate objections may no longer be processed.

In addition, data subjects have the right to object, without the need to provide any justification, to the processing of their personal data for direct marketing purposes in the name of the data controller or of a third party, or to the disclosure of such data to third parties for the same purposes.

In order to exercise their right to object, the data subjects must submit to the data controller a written, dated and signed request. In such request they may also indicate to the data controller an address where such information should be communicated to them.

5.5.2 Exceptions

The data subjects are not entitled to object to the processing of their personal data based on justified and legitimate reasons relating to their

particular situation when the law provides for exceptions from the possibility to exercise such right.

The same exception as for the information obligations applies (see section 4 above).

5.5.3 Deadline

The data subjects may exercise their right to object at any time. The data controller must communicate to the data subjects the measures taken in respect of the objection requests, and, if relevant, the name of the third parties to whom it has disclosed the data subjects' personal data within 15 days of the date it receives notification of the objection, and in the manner indicated by the data subjects, as mentioned in section 5.5.1 above.

5.5.4 Charges

The DPL provides that the data subjects' entitlement to exercise their right to object is free of charge only in respect of the processing of their personal data for direct marketing purposes in the name of the data controller or of a third party, or to the disclosure of such data to third parties for those purposes. However, in practice no charges are imposed on data subjects for any instances when they wish to object to the processing.

5.6 Automated individual decisions

5.6.1 Right

The data subjects are entitled to request and obtain: (i) the withdrawal or cancellation of any decisions producing legal effects on them and which have been made exclusively based on personal data processing through automated means, and are aimed at evaluating certain aspects of their personality; and (ii) the reassessment of any other decisions taken in respect of them, which materially affect them, provided that such decisions have been made exclusively based on personal data processing within the conditions mentioned under (i) above.

5.6.2 Exceptions

Data subjects do not benefit from the rights when the automated individual decisions are taken:

- within the context of the conclusion or execution of agreements, conditional upon the data subjects' request for the conclusion or execution of the agreements having been accepted, or certain adequate measures (such as the data subjects' possibility to claim their own opinion) to safeguard the protection of the data subjects' legitimate interests have been implemented; or
- if such decisions are authorised by laws providing for measures that safeguard the data subjects' legitimate interests,

but in all cases only if the other safeguards provided in the DPL are observed.

5.6.3 Deadline

The DPL is silent in respect of any deadlines.

5.6.4 Charges

The DPL is silent in this respect.

5.7 Other rights

5.7.1 Right

The data subjects are entitled to bring claims before the DPA (directly or indirectly, through representatives, including through associations or foundations) and the courts of law in connection with breaches of any of the rights guaranteed to them by such law.

In addition, data subjects benefit from the right that the DPA file claims before the courts of law, on their behalf, for the protection of any of the rights granted to them by the DPL.

5.7.2 Exceptions

There are no exceptions. However, a claim before the DPA may not be filed if a claim with the same object and envisaging the same parties has previously been filed before a court of law.

5.7.3 Deadline

Unless a delay would cause imminent and irreparable damage, a claim before the DPA may not be filed less than 15 days after the date a claim having the same object has been filed with the data controller.

In the case of claims for damages before the courts, the DPL does not provide for any specific deadline. Therefore, in this respect the general rules on civil liability in Romanian law will apply.

5.7.4 Charges

The data subjects' entitlement to exercise this right is free of charge.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The responsibility for notifying the DPA about the processing of personal data lies with data controllers.

6.1.2 What

As a general rule, any personal data processing operation (including transfers of data abroad) for a certain processing purpose, or any set of processing operations for the same or correlated processing purposes, must be notified separately from the DPA.

The DPA has published on its website a guideline on notification requirements and exemptions from it (the Notifications Guideline).

6.1.3 Exceptions

Personal data processing is exempt from the notification obligation if its sole

purpose is to keep a register which, by virtue of law, is intended to inform the public and is open to consultation by the public in general or by any person who proves a legitimate interest, conditional upon the processing being limited to the data which are strictly necessary to keep such register.

According to Decision of the President of the DPA No. 90/2006 of 18 July 2006 regarding the cases where it is not necessary to notify personal data processing and to Decision of the President of the DPA No. 100/2007 of 23 November 2007 for the establishment of the cases when the notification of the processing of certain personal data is not necessary (Decision 100/2007) notification is also not required, among others, for:

(i) processing of personal data of petitioners carried out by various public entities in order to achieve compliance with legal obligations;
(ii) employers' processing of personal data of their own employees and external collaborators in order to achieve compliance with legal obligations;
(iii) processing of personal data regarding the owners or lessees of a jointly used real estate property, which is done by the owners or lessees' associations in order to exercise their rights and obligations established by law for the management of such real estate;
(iv) processing of personal data carried out by the competent persons/departments of public/private entities in order to fulfil the obligations provided by law relating to the organisation and performance of the entity's own current economic-financial and administrative management;
(v) processing of personal data carried out for the subscription of shares in the interest of employees;
(vi) processing of personal data regarding members of associations, foundations or any other organisations without a patrimonial purpose, only for the purpose of fulfilling the entity's specific activity and provided that the personal data are not disclosed to third parties without the data subject's consent;
(vii) processing of personal data regarding contact persons of public or private entities, exclusively for the performance of professional and protocol activities, through the keeping of a record of contact data. As a rule, the exemption from notification under Decision 100/2007 also covers data transfers abroad, except for the categories of processing operations indicated at points (iv) and (vi) above, where a notification for the transfer abroad is still necessary.

Furthermore, simplified notification is allowed in certain cases mentioned in Decision No. 91/2006 of the President of the DPA regarding cases where simplified notification of personal data processing is allowed, which include cases where personal data are processed:

(i) by courts of law, local public administration, public and private education institutions, individuals and family associations performing authorised independent activities – to achieve compliance with some of their legal obligations;
(ii) for the purposes of managing the database kept by the National Archives;

(iii) by public and private entities, for lending books, cinema, artistic and other audiovisual masterpieces, as well as copies of them;
(iv) by public and private entities, for supplying gas, electricity, thermal energy, as well as water, sewage and salubrity, based on contracts concluded with clients;
(v) for intermediating real estate transactions.

6.1.4 When

Notifications to the DPA must be made prior to commencing the data processing operations.

The data controller must also notify to the DPA any change that may affect the accuracy of the information included in the notification (within five days from the date such change has occurred), the estimated date of completion of the personal data processing (by including this information in the notification form), as well as the exact completion date and the means of such completion (by updating the information provided in the submitted notification).

6.1.5 How

Notifications must be submitted by filling in a standard form approved by the Decision No. 95/2008 of the President of the DPA, for the establishment of the template form for the notifications provided by the DPL, which requires the provision of certain information, in line with the specific requirements provided in this respect by the DPL and the Directive. Certain additional information and documents may also have to be filed with the DPA attached to the notification (eg, sample information forms provided to data subjects, information on data processors, data transfer agreements).

From 1 October 2008, notifications must be first submitted using an online electronic application form which is available on the DPA's website. Notifications may be submitted only in Romanian. Within 30 days from the online submission of the notification, certain documents must be delivered to the DPA in paper format. The authority starts the review of the notification only after it receives these paper format documents, and it usually reverts within 30 days of such receipt by confirming the finalisation of the notification, or making comments, suggestions/asking for clarifications.

The data controller may generally start the notified processing operations after notifying the DPA about the intended processing, unless the authority's prior authorisation is required (see section 6.2 below). Although not explicitly provided by law, in practice the DPA requires that data controllers wait for its confirmation that the notification is complete, usually through registration of the notification with the Notifications Register, before starting the processing.

In 2009 the DPA received a total of 10,291 personal data processing notifications (representing an increase in the volume of notifications of more than 198 per cent compared with 2008). This includes 9,427 requests for registration of new notifications and 864 notifications regarding data

transfers abroad.

Statistics for 2010 and 2011 are not yet available.

6.1.6 Notification fees

As of 22 October 2007, notifications to the DPA are free of charge.

6.2 Authorisation requirements

Generally, data controllers do not need to obtain authorisation to carry out a data processing activity.

However, authorisation by the DPA is required in cases of intended:

(i) personal data processing operations which are deemed by law to pose specific risks to the rights and freedoms of data subjects. In this case, the data controller must notify the DPA about the processing at least 30 days before commencing it. Additionally, it may commence the processing either after the DPA performs a control and issues a decision authorising the processing/transfer (such decision must be issued within 30 days as of the notification's date), or five days after the registration of the notification with the DPA, if the data controller is not informed by the authority within such term about the authority's intention to perform its control.

(ii) transfers of personal data to countries which are deemed not to provide an adequate level of protection for the data subjects' fundamental rights (see section 8 below). In this case, the data controller may start performing the transfers only after obtaining transfer authorisation/s issued by the DPA. The law does not provide for a specific term within which transfer authorisations must be issued. However, if such transfers involve transmission of sensitive data and are not performed based on data transfer agreements concluded between the data controller and the foreign data recipient/s published by the European Commission (see section 8 below), the rules (including the terms) set forth by law in respect of the authority's prior control and authorisation in connection with the processing mentioned at point (i) above will also apply. The DPA issues authorisations for transfer on the basis of the notifications submitted by data controllers as described in sub-section 6.1 above.

6.3 Other registration requirements

Not applicable.

6.4 Register

At the end of the notification process the DPA registers the notification under distinct numbers in an online notifications register available for access on its website (the Notifications Register). This register may be consulted by anyone free of charge.

According to the DPL, data controllers must mention the data controller on each document through which the personal data contemplated in the notification are collected, stored or disclosed.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The DPL does not explicitly require the appointment of a data protection officer. However, legislation regulating specific fields such as internal affairs (police) requires the appointment of specialised departments or persons responsible for personal data protection (depending on the volume of personal data processing performed by data controllers in the field).

7.2 Tasks and powers

Under the legislation regulating internal affairs (police) the specialised departments/persons responsible for personal data protection have specific tasks and duties to ensure compliance with the applicable personal data protection legislation, including coordinating the preparation and implementation of procedures for personal data processing, to prepare a guideline regarding the exercise of the data subjects' rights, to coordinate and monitor personnel's activity in respect of personal data protection, etc.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

According to the DPL and the DPA's Decision No. 28 of 7 March 2007 on personal data transfers to other states, personal data transfers from Romania to EU/EEA member states and other states that have been officially recognised by the European Commission as providing an adequate level of protection for the fundamental rights of the data subjects are subject only to notification to the DPA.

Data transfers to other countries that have not been officially recognised by the European Commission as providing an adequate level of protection ('unsafe third countries') are generally subject, in addition to the notification obligation, to the requirement to obtain data transfer authorisation from the DPA.

8.2 Legal basis for international data transfers

As a general rule, personal data may be transferred from Romania to third countries which are deemed not to provide an adequate level of protection of data subjects' fundamental rights if the data controller provides sufficient safeguards with respect to the protection of the data subjects' fundamental rights. Such safeguards must be set forth in data transfer agreements concluded between the data controller and the recipients of the transferred data. The level of protection of the data subjects' fundamental rights is to be appreciated by the DPA by taking into consideration all the circumstances of the transfer, mainly the nature of the personal data subject to the transfer, the processing purposes, the proposed duration of processing, the country of export and the country of import and the legislation of the country of import.

The abovementioned rules, as well as the obligation to notify the DPA about an intended transfer of personal data abroad, are not applicable if: (i) the transfer is made based on a special law or on an international agreement ratified by Romania, particularly when the transfer is done for purposes of preventing, investigating or combating a criminal offence; or (ii) the

processing is done exclusively for journalistic, literary or artistic purposes, or the data have been made public manifestly by the data subject or are strongly connected with the data subject's status of public person or the public character of the deeds in which he is involved.

As an exception, personal data transfers to unsafe third countries are always allowed in any of the following cases explicitly provided in the DPL:

- the data subject has given his explicit consent to the intended transfer (where sensitive data are subject to transfer, such consent must be given in writing);
- the transfer is necessary for the performance of a contract concluded between the data subject and the data controller or for the implementation of certain pre-contractual measures taken pursuant to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controller and a third party, in the data subject's interests;
- the transfer is necessary for the achievement of a major public interest such as national defence, public order or national safety, for the good exercise of criminal trials or the ascertainment, exercise or defence of a right before court, provided that the data are processed in connection with such purposes and not for longer than is necessary;
- the transfer is necessary in order to protect the data subject's life, physical integrity or health;
- the transfer is made pursuant to a previous request for access to public official documents, or a request regarding information which may be obtained from registers or through any other documents accessible to the public.

8.2.1 Data transfer agreements

As a general rule, the use of data transfer agreements based on one of the European Commission's standard contractual clauses for data transfers to third countries is mandatory in Romania in order to obtain authorisation from the DPA for the transfer of personal data to countries which are deemed not to provide an adequate level of protection to the fundamental rights of the data subjects, when transfers are not based on the other grounds provided by the DPL. The use of such a data transfer agreement must be mentioned in the notification made to the DPA and a copy of the agreement must be submitted to the authority as attached to the notification (to the extent the notification is required by law).

8.2.2 Binding corporate rules

Romanian data protection legislation does not regulate the possibility to use binding corporate rules as a basis for personal data transfers to countries which are deemed not to provide an adequate level of protection to the fundamental rights of the data subjects. In addition, in its practice so far, the DPA has constantly refused to accept binding corporate rules as a basis of such transfers.

8.2.3 Safe Harbour

The DPA's authorisation is not required in respect of personal data transfers to organisations holding a valid certification under the US Safe Harbour scheme, provided that the transfer falls within the scope of application of such certification. However, the fact that the personal data transfer will be made based on a US Safe Harbour certification must be mentioned in the notification form submitted to the DPA in respect of the transfer.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The DPL requires data controllers and all persons acting on their behalf, including data processors, to ensure the confidentiality and security of personal data. In particular, such persons should process the personal data only on the basis of instructions received from the data controller, unless otherwise provided by law.

9.2 Security requirements

Data controllers and data processors must implement appropriate technical and organisational measures in order to protect personal data against accidental or unlawful destruction, or against loss, alteration, unauthorised disclosure or access, particularly if the processing entails data transmission through a network, as well as against any other unlawful form of processing.

These measures should ensure a level of security appropriate to the risks represented by the processing and the nature of the processed data, in accordance with the state of the art of the technique used in the processing process and the related costs. They also must comply with the minimum security requirements established by the DPA. Currently such minimum security requirements are provided in an order issued by the former DPA, ie, Order of the Romanian Ombudsman No. 52 of 18 April 2002 approving the minimum security requirements for personal data processing. According to this order, it is recommended that:

(i) users of personal data authenticate themselves and access only those personal data necessary for the fulfilment of their work duties;
(ii) data controllers appoint authorised users for collection and input of personal data into IT systems and for amendments to personal data;
(iii) back-up copies of databases containing personal data and of the programs used for automated personal data processing be made and stored in secured premises;
(iv) computers and other access terminals be installed in premises with restricted access;
(v) users of personal data be trained regarding the provisions of the DPL;
(vi) data controllers implement measures to protect the personal data processing against viruses;
(vii) data controllers approve specific internal procedures regarding the use and destruction of materials containing personal data, etc.

In 2006 the DPA posted on its web page for public consultation a draft normative decision for the approval of renewed minimum security

requirements for personal data processing, which contains requirements similar to those mentioned in the Romanian Ombudsman's Order No. 52/2002, as well as the requirement that data controllers establish their own written security policies and procedures and make them available to the authority upon request.

9.3 Data security breach notification obligation

Under the DPL there is no express obligation to notify personal data security breaches to the data subjects and/or to the DPA. Moreover, so far the DPA has not issued any recommendations in this respect.

9.4 Data protection impact assessments and audits

There is no legal requirement to carry out data protection impact assessments and audits as such under Romanian law. Moreover, the DPA has not issued any recommendations in this respect.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

In addition to its attributions mentioned in section 2.1 above, the DPA may carry out inspections on its own initiative or upon receipt of complaints, in respect of any breaches of data subjects' rights and of the data controllers and data processors' obligations within the context of personal data processing. However, the authority may not exercise its investigatory powers with respect to a breach if a claim with the same object and between the same parties has been previously brought before a court. Within its investigations, the DPA may:

(i) hear the data subjects, the data controllers, the data processors or the association or foundation representing the data subjects' rights;
(ii) request the data controllers to provide any information relating to personal data processing;
(iii) verify any document or record of the personal data processing; or
(iv) order examinations by experts.

In turn, the persons mentioned at point (i) above may submit complaints, documents and position papers. State secrecy and professional secrecy may not be alleged in order to impede the exercise of the authority's investigatory powers under the DPL.

Upon completing its investigations, the authority must issue a reasoned decision and communicate it to the concerned parties within 30 days from the date the authority received the complaint.

As mentioned in section 5.7.3 above, unless a delay would cause imminent and irreparable damage, a complaint before the DPA may not be filed within less than 15 days after the date a complaint having the same object has been filed with the concerned data controller.

10.2 Sanctions

Breaches of the rules provided by the Romanian data privacy legislation

may trigger the application of various sanctions including administrative fines, measures imposed by the DPA or by the courts of law in respect of the personal data processing operations and/or personal data which are unlawfully performed/processed, as well as the obligation to pay civil compensation for damages caused to persons in connection with the above-mentioned breaches.

Breaches of the rules provided in the DPL may qualify as minor offences triggering fines of up to approximately €12,000, unless conditions for the application of criminal liability are met. Data protection infringements have not yet led to criminal penalties being imposed. Under the current criminal legislation, criminal sanctions may be imposed for accessing correspondence of any kind without permission.

In addition, the DPA, pursuant to ascertaining breach of the data protection rules, may order the suspension or termination of all or part of the personal data processing operations, or the deletion of part or all of the processed data. The DPA publishes annually on its website information regarding the investigations performed and sanctions applied. In certain cases it also publishes on its web page information regarding particular investigations performed and the sanctions applied ('name and shame' approach).

10.3 Examples of recent enforcement of data protection rules

According to the DPA's 2009 activity report, the authority carried out 258 on-site controls in 2009. These included 251 investigations and seven prior controls the necessity of which was determined within the authority's review of submitted personal data processing notifications (see section 6.2 above). In four cases the authority requested that the personal data processing be ceased entirely or partly, while in seven cases it requested that the unlawfully processed data be deleted.

10.4 Judicial remedies

The DPA may file, free of charge, claims before the courts of law, for the protection of any rights guaranteed to the data subjects under the DPL.

In addition, as a general rule, data controllers and data subjects may file complaints against the DPA's decisions issued under the provisions of the DPL within 15 days from the date such decisions have been communicated to them.

10.5 Class actions

Class actions (ie, claims brought before the DPA and the courts of law by associations and foundations representing data subjects) are permitted under the DPL. So far, no such actions have been initiated.

10.6 Liability

In addition to submitting complaints before the DPA, data subjects may file civil claims before the competent courts of law if they think they incurred damage as a result of a data controller infringing their data protection rights. For example, in 2010 the Bucharest Tribunal ordered a local public authority

to pay to an individual €10,000 as damages for the unlawful publication on the authority's website of the individual's health data (ie, that he was suffering from AIDS). However, the case law in respect of claims related to data protection rights infringements continue to be limited.

In the case of claims for civil compensation for damages caused to persons in connection with the above-mentioned breaches, the persons against whom such claims are filed may be exonerated from liability by proving the occurrence of the general exonerating conditions provided by Romanian tort law.

In Romania, persons/legal entities processing personal data, as well as the data subjects are becoming more concerned about the personal data protection rules. However, so far there have been only limited cases where individuals have exercised their rights under the DPL. For instance, on 13 March 2009, Bucharest 1st District Court of First Instance ordered the City Hall of Bucharest's 1st District to pay moral damages of €10,000 to an individual whose personal data (including name, address, personal numeric code, details regarding the individual's health (ie that he was infected with HIV)) had been published on the City Hall's website in breach of confidentiality and the consent requirements provided by the DPL.

Slovakia

Havel, Holásek & Partners
Richard Otevrel & Jaroslav Šuchman

1. LEGISLATION

1.1 Name/title of the law

In addition to the international instruments protecting privacy (especially the European Convention for the Protection of Human Rights and Fundamental Freedoms) and personal data (particularly the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data), the basis for privacy protection is provided in Act No. 460/1992 Coll., Constitution of the Slovak Republic, of 1 September 1992, as amended.

In this context, Act No. 428/2002 Coll., on Personal Data Protection of 3 July 2002, as amended (the DPAct), serves as the implementing norm, both in relation to the abovementioned constitutional freedoms and to the Data Protection Directive 95/46/EC (the Directive). The DPAct provides for a general legal framework for the protection of personal data while any other laws and regulations function as exemptions from it, or provide for special regimes concerning particular types of personal data and means for processing them.

It is worth mentioning the following legislation that supports the overall system of data protection:

- Act No. 610/2003 Coll., on Electronic Communications, of 3 December 2003, as amended;
- Act No. 311/2001 Coll., Labour Code, of 2 July 2001, as amended;
- Act No. 40/1964 Coll., Civil Code, of 26 February 1964, as amended;
- Act No. 300/2005 Coll., Penal Code, of 20 May 2005, as amended.

1.2 Pending legislation

Currently, there is a pending government bill that will bring about an overhaul of the DPAct which is aimed at modernising, implementing relevant EU law, and streamlining some related processes (but which also causes political tensions due to some powers that the Office for the Protection of Personal Data (the Office) is trying to obtain under this bill). One of the changes that will be enshrined into the law is the current practice of the Office and its related interpretation of the DPAct, which does not require the Office's approval for a transfer of data to third countries in controller-controller scenarios.

There is also a draft of the Act on Electronic Communications, which implements the respective provisions of Directive 2009/136/EC, which amended the ePrivacy Directive, that are under discussion. It has been

approved by the government and is now in the National Council. The act is scheduled to become effective as of 1 October 2011, subject to the approval of the National Council.

The draft law includes the wording of the revised Article 5(3) of the Directive, plus some elements of recital no. 66, which recognise the possibility of obtaining consent via browser settings or settings of other software. In its proposed form, it legally requires opt-in affirmative consent given prior to processing and based on clear and complete information regarding the purpose of the processing.

1.3 Scope of the law

1.3.1 The main players

- The 'controller' means a state administration authority, territorial self-government authority, or other public authority body, or legal or natural person, who alone, or jointly with others, determines the purposes and means of processing personal data. Where the purposes and means of the processing of personal data are regulated by a special act, the controller is thereby the authority determined for the fulfilment of the purpose of the processing, or the authority which fulfils the requirements stipulated by law.
- The 'processor' means a state administration authority, territorial self-government authority, other public authority body or other legal or natural person processing personal data on behalf of the controller or the controller's representative.
- The 'data subject' means any natural person whose personal data are processed. 'Personal data' means any information related to an identified or identifiable natural person, while such a person is one who can be identified, directly or indirectly, in particular by reference to an identifier of general application, or by reference to one or more factors specific to his physical, physiological, psychic, mental, economic, cultural, or social identity.
- The 'third party' is a state administration authority, territorial self-government authority, other public authority body, or any legal or natural person other than the data subject, controller, or controller's representative, his processor, and their entitled persons.

1.3.2 Types of data

The DPAct only covers personal data related to natural persons, as opposed to data relating to legal persons (eg, companies).

Given the definition of 'personal data' in section 1.3.1 above, it includes, eg, an individual's name, address, photograph, telephone number, bank account number, etc.

The DPAct distinguishes between a general category of personal data and special categories of personal data. The special categories include:

(i) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of political parties or movements, trade union membership, and data concerning health or sex life

(processing of these data is generally prohibited);
(ii) data in the form of an identifier of general application stipulated by a special law (it may be used for the purposes of identification of a natural person, only provided that its use is necessary for achieving the given purpose of processing, while processing a different identifier revealing characteristics of the data subject, or releasing an identifier of general application, is prohibited);
(iii) data relating to a breach of provisions of the Penal Code, the Misdemeanours Act, or Civil Code, or relating to the execution of final judgments or decisions (which may only be processed by a person entitled to do so by a special law);
(iv) biometrical data (which may only be processed under conditions stipulated by a special law, provided that it expressly ensues from a statutory provision or that the data subject gave written consent to the processing);
(v) data relating to the mental identity of a natural person or his mental capacity to work (which may only be processed by a psychologist or by a person entitled to it by a special law).

'Anonymous personal data' are personal data adjusted in such a manner that they cannot be matched with the concerned data subjects; anonymous data are not subject to the DPAct Any method that would enable, wholly or partially, the reconstruction of the link between data and data subject would mean that the data were no longer anonymous and render them subject to the DPAct.

1.3.3 Types of acts/operations

The DPAct covers the 'processing' of personal data, defined as any operation or set of operations which is performed upon personal data, such as obtaining; collecting; recording; organising; adapting or altering; retrieving; consulting; aligning; combining; transferring; using; storing; destroying; transmitting; providing; making available; or making public. The DPAct applies to personal data systematically processed by fully or partially automated means, or by means other than automated means of processing, which constitute part of a filing system, or are intended to be processed in a filing system. A 'filing system' is any structured set, system or database containing personal data, which are systematically processed to achieve a purpose according to specific criteria and conditions, while using automated, partially automated or other than automated means of processing, disregarding whether the system is centralised, decentralised, or dispersed on a functional or geographical basis (eg, card index, list, register, file, record, or a system containing files, documents, contracts, certificates, references, assessments, tests).

1.3.4 Exceptions

Personal data processed by a natural person for his own needs within the framework of purely personal or household activities – such as keeping a personal directory or correspondence – or personal data that are obtained

accidentally without prior determination of a purpose and means of processing, without the intent of their further processing in an organised system, fall outside, and are not protected under, the DPAct.

Moreover, partial exemptions exist for the following types of data processing required by specific laws for securing public interest, provided that the controller fulfils the obligations expressly stipulated by a special law in order to safeguard:

(i) the security of the Slovak Republic;
(ii) the defence of the Slovak Republic;
(iii) public policy and security;
(iv) the preventing, precluding, detecting, and documenting of criminal offences, disclosing their perpetrators, investigating and prosecuting of criminal offences;
(v) the important economic or financial interests of the Slovak Republic or of the European Union, including monetary, budgetary and taxation matters;
(vi) inspection, internal supervision, external supervision, or regulatory function connected with the exercise of the official authority in cases under (iii), (iv), and (v); or (vii) protection of the data subject, or of the rights and freedoms of others.

1.3.5 Geographical scope of application

The following two categories of data processing operations fall within the geographical scope of the application of the DPAct:

- The processing of personal data carried out by state administration authorities, territorial self-government authorities, and other public authority bodies, as well as by other legal and natural persons who process personal data, determine the purpose and means for processing or provide personal data for their processing.
- The processing by controllers who do not have a registered office or permanent residence in the territory of the Slovak Republic but are located abroad at a place where the laws of the Slovak Republic take precedence based on international public law, or are located in a member state of the European Union, provided that, for the purposes of personal data processing, they fully or partially use automated means or other than automated means, for processing located in the territory of the Slovak Republic, while such means of processing are not used solely for the transfer of personal data through the territory of the member states of the European Union. In such a case, the controller shall proceed pursuant to a special provision of the DPAct (demanding, the nomination of a local representative in Slovakia).

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Úrad na ochranu osobných údajov Slovenskej republiky (The Office for the

Protection of Personal Data of the Slovak Republic)
Odborárske námestie c. 3
817 60 Bratislava 15
Slovak Republic
T: +421 2 502 39 418
F: +421 2 502 39 441 (President of the Office)
+421 2 502 39 440 (Chancery of the chief inspector)
E: statny.dozor@pdp.gov.sk
W:*www.dataprotection.gov.sk*

2.1 Role and tasks

The Office for the Protection of Personal Data of the Slovak Republic (the Office) is an independent body and its primary objective is to ensure that every individual's right to privacy is protected in the context of personal data processing.

2.2 Powers

The Office has the following general competences:

- to continuously inspect the state of protection of personal data; to register the filing systems; and to keep the records concerning the filing systems;
- to recommend to controllers measures for ensuring the protection of personal data in the filing systems; for this purpose, it issues recommendations to controllers within the scope of its power;
- to issue a binding decision in case of doubt regarding the extent, content, and manner of processing, as well as whether the use of the processed personal data are adequate for the purposes of their processing, whether they are compatible with the respective purposes for the processing, or whether they are up-to-date with regards to the time and subject matter for this purpose;
- to issue a binding decision in case of doubt regarding cross-border personal data flow;
- to issue a binding decision in case of doubt regarding the registration of a filing system;
- to investigate reports, or proceed upon an instigation of its own initiative, and issue measures for the removal of defects;
- in case of suspicion that obligations imposed by the DPAct were breached, it may summon the controller or the processor and request an explanation;
- to inspect the processing of personal data in the filing systems;
- to impose sanctions determining that the obligations referred to in the DPAct were breached;
- to notify law enforcement agencies in case of a suspicion that an offence was committed;
- to register filing systems and provide access to the registration;
- to participate in drafting generally binding legal regulations in the field of personal data protection;

- to issue generally binding legal regulations within the scope of its power;
- to give opinions on draft laws and other generally binding legal regulations, which regulate the processing of personal data;
- to submit to the National Council of the Slovak Republic a report on the state of the protection of personal data at least once every two years.

The most significant power that the Office has is that it may carry out on-site investigations. In the course of inspection activities, the chief inspector and other inspectors ('inspection authority'), who are part of the Office and nominated by the government for a five-year period, as well as the President of the Office and the Vice-President of the Office, are entitled to:

- enter the lands, buildings, or premises of the operations and facilities of the controller and of the processor;
- request from the controller, processor, and their employees ('inspected person') to provide them, within a determined time limit, with documents and other papers, opinions, and information, data processed on storage media, including technical data carriers, reports, and source codes for programs, provided that they own them, and other records necessary for the execution of the inspection, originals or copies, and to enable them, in justified cases, to also make copies outside the premises of the inspected person;
- request from the inspected person to provide, within a reasonable time limit, complete and true oral and written information, opinions, and explanations with respect to the inspected and related facts and determined deficiencies;
- require cooperation of the inspected person;
- access the filing systems as the system administrator to the extent necessary for performing the inspection;
- verify the identity of the inspected persons and the natural persons acting on behalf of the inspected persons.

2.3 Priorities

As indicated in the latest annual reports, the Office currently prioritises finding adequate means to balance the need to secure the interests of individuals with sufficient practicability regarding personal data processing in information systems. The Office has declared that it will put an emphasis on preventative action – the preferred reaction to a determined breach of the DPAct being the imposition of remedial measures rather than financial sanctions.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Consent constitutes one of the possible legal bases for the processing of general personal data and some of the special categories of data, if not ruled out by a special act.

The data subject's 'consent' is defined as 'any freely given specific and informed indication of his wishes by which the data subject knowingly

signifies his agreement that personal data related to him may be processed'.

3.1.2 Form

In principle, the DPAct does not require consent to be given in a specific form. However, the processing of personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; membership of political parties or movements; trade union membership; data concerning health or sex life; and biometrical data is only possible upon written consent.

If the controller processes personal data with the consent of the data subject, he is obliged to prove to the Office, anytime upon request, that he has obtained such consent. The DPAct explicitly provides for forms of proof of consent. The consent can be proved by an audio or audiovisual recording, or by an affidavit from the person that provided the personal data to the filing system, or in another reliable manner.

3.1.3 In an employment relationship

Consent must be given freely. In an employment relationship it may be questioned whether the subordinate position of an employee prevents consent from being truly 'free', especially when the Labour Code provides for a limit on the extent of personal data that an employer may process – the employer may only request such data that relate to the qualifications or professional experience of the employee, and that are, or may be, relevant to the work position of the particular employee.

3.2 Other legal grounds for data processing

The basic premise of the DPAct is that personal data may only be processed upon the consent of the data subject, unless otherwise stipulated by the DPAct.

Other grounds for processing without consent include:

- Where necessary for the purposes of artistic or literary expression and for the purposes of informing the public by means of the mass media. In both cases the personal data can only be processed by a controller for whom such processing falls in the scope of his activities. This does not apply if, by processing personal data for such a purpose, the controller violates the data subject's right to the protection of his personal rights and privacy, or if such processing of personal data without consent of the data subject is prohibited by another law or an international treaty that is binding on the Slovak Republic.
- Where necessary for the performance of a contract to which the data subject is party, or in order to establish relations or take steps at the request of the data subject prior to entering into a contract.
- Where necessary for the protection of life, health, or property of the data subject, or of another natural person, without the legal capacity or physical ability to give consent and where consent of his legal representative cannot be obtained.
- When the data solely consist of the title, name, surname, and address

of the data subject and are to be used solely for the controller's needs concerning mail correspondence with the data subject and keeping records of such data. If the scope of the controller's activities includes direct marketing, he may transmit the above personal data, without making them available and public, only if they are to be transmitted to another controller whose scope of activity is also direct marketing and the data subject did not file an objection in writing.

- Prior publicity of processed personal data – in such cases, personal data must be duly denoted.
- Where necessary for the fulfilment of an important task carried out in the public interest.
- Where necessary for the protection of statutory rights and legitimate interests of the controller or the third party, provided that when processing such personal data the controller and the third party respect the fundamental rights and freedoms of the data subject and, by their conduct, do not violate his right to protection of his personal rights and privacy.

Processing the special categories of personal data mentioned in section 1.3.2 above is, in principle, prohibited unless the processing meets certain specific requirements. In particular, personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; membership of political parties or movements; trade union membership; and the processing of data concerning health or sex life may be processed if the data subject has given his written consent, or if:

- the processing is required by a special law stipulating a list of personal data, the purpose of their processing and the group of data subjects. The processed personal data of the data subject may be provided, made available, or made public only if the law stipulates the purpose of the provision; or the list of personal data that can be provided as well as the third parties to whom the personal data are provided, or a group of recipients to whom personal data are made available, unless otherwise stipulated by the DPAct; or
- the processing is necessary for the protection of vital interests of the data subject or of another natural person without the legal capacity or physical ability to give consent, and where the consent of his legal representative cannot be obtained; or
- the processing is performed within the framework of legitimate activities by a civil society, foundation, or non-profit organisation providing generally beneficial services; by a political party or movement, trade union organisation, church or religious society acknowledged by the state, and such processing only concerns their members, or the natural persons with whom they are in a regular contact with respect to their objectives, and the personal data serve solely their internal needs and will not be provided to a third party without the written consent of the data subject; or
- the processing concerns personal data which have already been made public by the data subject, or which are necessary for exercising a legal

claim; or
- the processing is performed for the purposes of providing medical care and affecting public health insurance, provided that these data are processed by a provider of the medical care, a health insurance company or the Office for Internal Supervision over Health Care; or
- the processing is performed within the framework of social insurance or social security of policemen and soldiers, for the purposes of providing social relief or assistance in distress, or if the processing is necessary for the purposes of fulfilling obligations or exercising the legitimate rights of the controller responsible for the processing in the field of labour law and employment services, and if it ensues from a special law.

3.3 Direct marketing and cookies

For direct marketing, the processing of personal data is subject to the general provisions of the DPAct. In addition, the DPAct contains specific provisions on direct marketing.

No consent is needed if the personal data consist of solely the title, name, surname, and address of the data subject, and where the data are to be used solely for the controller's needs concerning mail correspondence with the data subject and keeping records of such data. If the scope of the controller's activities is direct marketing, he may provide the above personal data, without making them available and public unless they are to be provided to another controller whose activity is also solely direct marketing and the data subject did not file an objection in writing which must be free of charge.

In addition, Act No. 610/2003 Coll., on Electronic Communications, of 3 December 2003 contains provisions that protect consumers against unsolicited advertisements.

The use of cookies or equivalent devices is regulated by the Act on Electronic Communications. There is a new bill on Electronic Communications being debated in the National Council that should implement the respective provisions of Directive 2009/136/EC, which has amended the ePrivacy Directive. The act is scheduled to become effective as of 1 October 2011, subject to the approval of the National Council.

The draft law includes the wording of revised Article 5(3) of the ePrivacy Directive, as well as some elements of recital no. 66, which recognise the possibility of obtaining consent via browser settings or via the settings of other software. In its proposed form, it legally requires opt-in affirmative consent, given prior to processing, and on the basis of clear and complete information regarding the purpose of the processing.

Under the current law, in principle, the use of electronic communications networks to store cookies or equivalent devices on a user's or a subscriber's terminal equipment is only permitted if: (i) the user or subscriber has been informed of the purposes of the data processing and of his rights; and (ii) the controller has offered the user or subscriber the possibility of opting out before installing the cookies.

3.4 Data quality requirements

Controllers must ensure the fair and lawful processing of personal data.

Personal data must be collected for specified, explicit, and legitimate purposes, and may not be further processed in a manner that is incompatible with those purposes.

Moreover, only personal data that are accurate, relevant, not excessive in relation to the purposes for which they are collected and/or further processed, kept up to date, and kept in a form permitting the identification of data subjects for no longer than necessary, may be processed.

3.5 Outsourcing

When outsourcing data processing activities to processors, the controller must be mindful of guarantees in the field of technological, organisational, and personal security measures. The controller may not entrust personal data processing to a processor if that could present a risk to the rights and statutorily protected interests of the data subjects. The controller is required to select a processor who will take the necessary security measures, supervise the processor's compliance with these security measures, and enter into a written agreement with the processor or provide him with written authorisation. The processor shall only be entitled to process personal data to the extent and under conditions agreed upon with the controller, or with another processor, provided that the controller gives consent to it in a written contract or written authorisation.

If the controller outsourced to the processor after acquiring personal data, he should inform the data subjects of this fact during their next contact, or not later than three months from the day of outsourcing the task to the processor. This will also be needed when data processing is taken over by another controller.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use, as well as the use of surveillance cameras, is subject to the provisions of the DPAct.

In addition, the Act on Electronic Communications (see section 1.1 above) contains important restrictions on intercepting electronic communications during a transfer, which not only apply to listening in on telephone conversations, but also to monitoring email messages before they reach the recipient. In addition, this Act imposes specific obligations for accessing information stored on a user's computer (or other equipment) using an electronic communications network.

Premises accessible to the public may be monitored by means of video recording (or audio recording) only for the purposes of public policy and security, disclosing criminal activities, or interfering with state security, provided that the premises are clearly marked as being monitored. Providing on-site information on monitoring of premises is not required if it is not stipulated by a special law. The recording made may only be used for the purposes of criminal prosecution or for proceedings that concern misdemeanours, unless otherwise stipulated by a special law.

3.6.2 Employment relationship

According to the Labour Code, the employer may not invade the employee's privacy, especially by open or covert monitoring, wiretapping, or searching of regular mail addressed to the employee, unless it is substantiated by 'specific activities of the employer'. The employee must be informed of such monitoring (the method and extent) in advance.

In addition, for the purpose of the protection of its own property, the employer is entitled to implement (and adopt as internal rules) necessary measures for monitoring things that the employee brings into or out of the workplace (such monitoring must not affect human dignity and the general principles of privacy protection must be adhered to during the conduct of such monitoring). At this moment, no further guidance has been developed by case law and it is probable that the European Court of Human Rights' rulings would be applied primarily to set a frontier between an employee's privacy and an employer's right to pursue his supervision.

4. INFORMATION OBLIGATIONS

4.1 Who

Controllers are responsible for informing the data subjects of the processing of personal data that relate to them.

4.2 What

The controller who intends to obtain personal data from the data subject shall be obliged to inform the data subject, at the latest, when obtaining the data, and notify him of the following:

(i) the name and registered office or permanent residence of the controller; if in the territory of the Slovak Republic, the controller's representative acts on behalf of the controller, which has its registered office or permanent residence in a third country, the controller's representative shall also notify the data subject of the name and registered office or permanent residence of the controller;
(ii) the name and registered office and permanent residence of the processor, provided that the processor obtains the personal data on behalf of a controller or a controller's representative; and
(iii) the purpose of the personal data processing.

Additional information should be provided to the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data, in particular, with regard to the right to be informed about conditions of the processing of his personal data, including:

- identification of the person obtaining the personal data;
- advice on the obligation to provide the requested personal data. If the data subject can decide on the provision of his personal data, the controller shall notify the data subject on what legal basis he intends to process the data subject's personal data; if the obligation of the data subject to provide his personal data arises from a special law, the controller must inform the data subject of which law imposes

this obligation on the data subject, and warn the data subject of the consequences of refusing to provide the personal data;
- third parties or a group of recipients (a sub-group of third parties who receive data), provided that it is expected or clear that the personal data will be provided to them;
- form of making public, provided that the personal data are to be made public;
- third countries, provided that it is expected or clear that the personal data will be transmitted to these countries;
- advice on the existence of the data subject's rights.

If the controller did not obtain the data subject's personal data directly from the data subject, he must notify the data subject of all the information under (i) to (iii) above and of additional information to the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all the circumstances of the data processing, and in particular, with regard to the right to be informed about conditions of the processing of his personal data, including:
- advice on the possibility to decide to process the obtained personal data;
- list of personal data;
- third parties, provided that it is expected or clear that the personal data will be provided to them;
- group of recipients, provided that it is expected or clear that the personal data will be made available to them;
- form of making public, provided that the personal data are to be made public;
- third countries, provided that it is expected or clear that the personal data will be transmitted to these countries;
- advice on the existence of the data subject's rights.

Upon written application, the data subject is entitled to request from the controller:
- name, registered office or permanent residence, corporate form, and identification number of the controller;
- name and surname of the statutory authority of the controller;
- name and surname of the personal data protection official performing the internal supervision of personal data protection (see section 7 below), provided that his appointment is required;
- name, registered office or permanent residence, corporate form, and identification number of the controller's representative, provided that he acts on the territory of the Slovak Republic on behalf of the controller, who has his registered office or permanent residence in a third country;
- name and surname of the statutory authority, or member of the statutory authority of the controller's representative;
- identifier of the filing system;
- purpose of the processing of the data;
- list of the personal data;
- group of data subjects;

- group of recipients, provided that it is expected or clear that the personal data will be made available to them;
- third parties or a group of third parties, provided that it is expected or clear that the personal data will be provided to them;
- third countries, provided that it is expected or clear that the personal data will be transferred to these countries and the legal basis of the cross-border flow;
- legal basis of the filing system;
- the form of making public, provided that the personal data are to be made public;
- general characteristics of the measures for ensuring protection of the personal data; and
- date of commencement of the processing of the personal data.

The controller is exempt from providing the above information if:

- the data subject is already aware of the information; or
- recording or disclosing of the data is expressly laid down by law.

4.3 When

The information should be provided at the time the personal data are recorded. When the data are not obtained directly from the data subject, the information should be provided at the time when the personal data are recorded, or when a disclosure to a third party is envisaged, but no later than the first time the data are disclosed.

4.4 How

The DPAct does not specify in what form and how the information must be provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Upon written application, the data subject is entitled to request from the controller:

- information about the state of the processing of his personal data in the filing system in a generally intelligible form;
- exact information, in a generally intelligible form, about the source from which the controller obtained his personal data for processing;
- a copy of the personal data, in a generally intelligible form, which constitute the subject of the processing;
- rectification of inaccurate, incomplete, or out-of-date information, which constitute the subject of the processing;
- destruction of his personal data, provided that the purpose of their processing has ceased;
- destruction of his personal data, which constitute the subject of the processing, provided that the law was breached.

5.1.2 Exceptions

The right to access may, under no circumstances, be refused, although the rectification or destruction may be limited by a special act or if third party rights would be infringed (such a limitation must be notified to the data subject).

5.1.3 Deadline

The data subject can exercise his right to access at any time. In response, the controller must communicate the information within 30 days after the receipt of the request.

5.1.4 Charges

The data subject generally may not be charged for exercising his right to access. The information on the source from which the controller obtained his personal data for their processing, and a copy of personal data which constitute the subject of the processing, may be charged in the amount not exceeding the amount of material costs accrued in connection with making the copies, providing the technical carriers, and sending the information to the data subject, unless otherwise stipulated by a special law.

5.2 Rectification

5.2.1 Right

Any data subject has the right to obtain from the controller the rectification of inaccurate, incomplete, or out of date personal data relating to him.

5.2.2 Exceptions

The rights of the data subject regarding rectification may be restricted provided that such a restriction results from a special law or, if the exercising of this right would infringe the protection of the data subject or the rights and freedoms of others.

5.2.3 Deadline

The controller must notify the data subject, and every person to whom he provided personal data, of the rectification or destruction of the personal data within 30 days from its execution. No notification is necessary provided that the rights of the data subject are not violated by it.

5.2.4 Charges

The data subject may not be charged for exercising his right to rectification.

5.3 Erasure

5.3.1 Right

Any data subject has the right to seek the destruction of his personal data, provided that the purpose of their processing was fulfilled; if any official documents containing personal data constitute the subject of the processing, he may request their return. The data subject also has the right to seek the destruction of his personal data, which constitute the subject of the processing if the law is breached.

5.3.2 Exceptions

The rights of the data subject regarding destruction may be restricted if such a restriction results from a special law, or if exercising this right infringes the protection of the data subject or the rights and freedoms of others.

5.3.3 Deadline

If the data subject's request is justified, the controller must erase the personal data without undue delay. The controller shall notify every person to whom he provided the personal data of the destruction, without undue delay and in writing. A ban on further transmission/disclosure of the personal data will apply to the controller and to every person to whom the controller provided the personal data, from the day after the day of delivery of the data subject's objection, or after the day of the delivery of the controller's notification in writing.

The controller shall notify the data subject, and every person to whom he provided personal data, of the rectification or destruction of the personal data within 30 days from its execution. Notification is not necessary if the rights of the data subject are not violated by it.

5.3.4 Charges

The data subject may not be charged for exercising his right to erasure.

5.4 Blocking

5.4.1 Right

There is no explicit right to demand blocking, but the controller is obliged to block personal data, the processing of which was objected to by the data subject, without undue delay, and destroy them as soon as possible.

5.4.2 Exceptions

There are no exceptions to the blocking right.

5.4.3 Deadline

The controller must act without undue delay.

5.4.4 Charges

The data subject may not be charged for exercising his blocking right.

5.5 Objection

5.5.1 Right

A data subject is entitled to object to the controller, upon a free-of-charge written application, to the following:

- processing of his personal data, with respect to which he expects that they are or will be processed for the purposes of direct marketing without his consent – he can seek their destruction;
- use of the personal data for the purposes of direct marketing in mail correspondence; or
- transmission/disclosure of personal data for the purposes of direct

marketing.

Furthermore, provided that the matter cannot be postponed, a data subject is entitled to object to the processing of personal data to the controller, at any time, personally or upon a free-of-charge written request, by stating any legitimate reasons, or by submitting evidence of the infringement of his rights and legitimate interests that are, or may be, violated by the processing of personal data in a concrete case. If it is proved that the objection of the data subject is valid, and no legitimate reasons prevent it, the controller must block the personal data, the processing of which was objected to by the data subject, without undue delay, and destroy them as soon as possible.

5.5.2 Exceptions

The data subject can be deprived of the right to object only if it ensues from a special law which provides for measures to secure the legitimate rights of the data subject.

No exceptions apply with respect to the right to object to the processing of personal data for direct marketing purposes.

5.5.3 Deadline

If it is proved that the objection by the data subject is valid, and that legitimate reasons do not prevent it, the controller must block the personal data, the processing of which was objected to by the data subject, without undue delay and destroy them as soon as possible.

The controller must stop the processing of personal data for direct marketing purposes upon the data subject's objection.

5.5.4 Charges

The data subject may not be charged for exercising the right to object.

5.6 Automated individual decisions

5.6.1 Right

The data subject is entitled to object to the controller, at any time, personally or upon a free-of-charge written request, provided that the matter cannot be postponed, and can refuse to submit to the controller's decision, which would produce legal effects on him, or significantly affect him, provided that such a decision is based solely on the acts of the automatic processing of his personal data. The data subject may request from the controller the examination of the issued decision by a method other than automatic processing, while the controller shall be obliged to satisfy the request of the data subject in such a manner that the entitled person (the person authorised to work with the data) shall have a decisive role in the examination of the decision.

5.6.2 Exceptions

The data subject can be deprived of the above right only if so stipulated by a special law that includes measures to secure the legitimate rights of the data

subject, or if the above decision was made in the course of the entering into, or performance of, a contract between the controller and the data subject, under the condition contained in the contract that the request of the data subject was satisfied, or that the data subject was granted the right, based on an agreement, to demonstrate his point of view at any time during the contract's validity.

5.6.3 Deadline

The controller must inform the data subject about the manner of examination and the outcome of his finding within 30 days.

5.6.4 Charges

The data subject may not be charged for exercising his right.

5.7 Other rights

5.7.1 Right

The data subject is entitled to disagree with the controller's decision, and to refuse the transfer of his personal data to a third country which does not ensure an adequate level of protection of personal data.

If the data subject suspects that his personal data are processed without authorisation, he may notify the Office of such a suspicion.

If the data subject does not enjoy full legal capacity, his rights may be exercised by his legal representative.

If the data subject is not alive, his rights arising from DPAct may be exercised by a 'close person'.

5.7.2 Exceptions

There are no exceptions.

5.7.3 Deadline

Not applicable.

5.7.4 Charges

The data subject may not be charged for exercising these rights.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The controller must submit the filing system for registration before the commencement of the processing of the personal data.

6.1.2 What

The obligation to register applies to all filing systems in which personal data are processed by fully or partially automated means of processing.

6.1.3 Exceptions

The following filing systems are exempt from registration:

- those that are subject to internal supervision of a personal data protection official, who was authorised, in writing, by the controller and who executes the internal supervision of personal data protection pursuant to the DPAct;
- those containing personal data of natural persons processed for the purposes of fulfilling pre-contractual relations or for the purposes of exercising the rights and obligations resulting, for the controller, from an existing or terminated employment relationship, civil service relationship, civil service employment relationship, or membership relation with these natural persons, including the personal data of their 'close persons';
- those containing personal data concerning the membership of the persons in a trade union and, if these personal data are processed by the trade union and used solely for its internal needs, or containing personal data concerning religious beliefs of persons associated with a church, or religious association acknowledged by the state, and if these personal data are processed by the church or the religious association, and used solely for their internal needs, or containing personal data concerning the membership of persons in a political party or movement, and if these personal data are processed by the political party or movement and used solely for their internal needs; or
- containing personal data necessary for exercising the rights or fulfilling the obligations arising from a special law, or which are processed pursuant to a special law.

6.1.4 When

Notification must be made prior to starting any automated processing activity.

6.1.5 How

The Office assigns a registration number to the filing system and confirms the registration. However, the processing is not conditioned by the issuance of a confirmation of the registration. The registration information must be submitted, in writing, to the Office by the controller, or electronically, in the form of a database file with an attached print copy of the contents of the file confirmed by the controller.

6.1.6 Notification fees

Registration is free of charge.

6.2 Authorisation requirements

In principle, controllers do not need to obtain authorisation to carry out data processing. However, authorisation may be required for the transfer of personal data for processing abroad (see section 8).

6.3 Other registration requirements

There is a so-called 'special registration' that applies to filing systems, in

which the controller processes:

- at least one of the following personal data: racial or ethnic origin; political opinions; religious or philosophical beliefs; membership in political parties or movements; trade union membership; and the processing of data concerning health or sex life; and, at the same time, their transfer to a third country or third countries not ensuring an adequate level of protection is expected or executed;
- personal data necessary for the protection of statutory rights and legitimate interests of the controller or the third party, provided that, in such processing of personal data, the controller and the third party respect the fundamental rights and freedoms of the data subject; or
- biometrical data.

The Office shall assess the submitted data, verify whether the processing of the personal data could infringe the rights and freedoms of the data subjects, and decide, within 60 days from the day of their receipt, whether it will permit the processing of the personal data. In case of any doubts, the Office may also request further explanations and/or documents from the controller.

6.4 Register

The Office runs two registers, the register of filing systems (all filing systems, in which personal data are processed by fully or partially automated means of processing) and the special register (for filing systems processing the described special categories of data). It is accessible at *www.dataprotection.gov.sk/buxus/generate_page.php?page_id=140*. The required information for registration includes: name, registered office or permanent residence, corporate form and identification number of the controller; name and surname of the statutory authority of the controller; name and surname of the personal data protection official performing internal supervision of personal data protection, provided that his appointment is required; name, registered office or permanent residence, corporate form and identification number of the controller's representative; name and surname of the statutory authority or member of the statutory authority of the controller's representative; identifier of the filing system; purpose of the processing of personal data; list of personal data; group of data subjects; group of recipients, provided that it is expected or clear that the personal data will be made available to them; third parties or a group of third parties, provided that it is expected or clear that personal data will be provided to them; third countries, provided that it is expected or clear that personal data will be transferred to these countries and the legal basis of the transborder flow; legal basis of the filing system; the form of making public, provided that personal data are to be made public; general characteristics of the measures for ensuring protection of personal data; and the date of commencement of the processing of personal data.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

If the controller employs more than five persons, he must designate a personal data protection official or several personal data protection officials. The controller may designate a personal data protection official if he employs less than six persons. He must provide professional training in the area of personal data protection to the designated official(s). The controller who authorised the personal data protection official must notify the Office, in writing, by means of a registered letter, without undue delay, and at the latest within 30 days from the day of the authorisation of the personal data protection official.

For a controller employing fewer than six employees, the advantage in designating an official lies in the release from the obligation to register the processing with the Office.

7.2 Tasks and powers

The official supervises the observation of the statutory provisions in the processing of personal data. He provides:

- the necessary cooperation with the Office in fulfilling the tasks within his scope of power;
- assessment as to whether any danger of violation of the rights and freedoms of the data subjects arises from the processing of personal data;
- internal supervision of the fulfilment of the controller's basic obligations;
- advice to the entitled persons working with personal data (natural persons disposing of personal data within the framework of employment relationship, civil service employment relationship, civil service relationship, membership, based on authorisation, election or appointment or within the framework of performance of a public office, who may process personal data only upon instruction of the controller, controller's representative or processor);
- assessment and resolution of issues raised by applications of the data subjects regarding the data processing;
- implementation of technical, organisational and personal security measures and the supervision of their application in practice;
- internal supervision of the selection of processors and the drafting of a written contract or written authorisation for the processors, and taking responsibility for its contents;
- internal supervision of cross-border personal data flow;
- submission of filing systems for special registration with the Office.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Data transfers between the Slovak Republic and EU member states are unrestricted.

Data transfers to countries outside the EU that provide an adequate level of protection are possible under the condition that the data subject was provided with the necessary information, or under certain other conditions.

Personal data may be transferred to a third country that does not ensure

an adequate level of protection only under certain conditions (see below).

8.2 Legal basis for international data transfers

Personal data may be transferred to a third country that does not ensure an adequate level of protection on the basis of a decision of the European Commission, or if any of the following conditions are fulfilled:

- the data subject gave written consent to it, while knowing that the country of the final destination does not ensure an adequate level of protection;
- it is necessary for the performance of a contract between the data subject and the controller;
- it is necessary for the entering into, or performance of, a contract, concluded by the controller, in the interest of the data subject with another entity;
- it is necessary for the performance of an international treaty binding the Slovak Republic, or resulting from the laws due to an important public interest, or for the proving, filing, or defending of a legal claim;
- it is necessary for the protection of the vital interests of the data subject; or
- it concerns the personal data, which constitute part of the lists, registers, or files and are kept and publicly accessible pursuant to special laws, or are available, under these laws, to the persons who prove a legal claim and fulfil the conditions prescribed by law for making them available.

8.2.1 Data transfer agreements

Authorisation for the transfer of personal data to a third country is not required unless the controller entrusts an entity residing abroad with the processing of the personal data on the controller's behalf. This entity may process the personal data only to the extent and under conditions agreed upon with the controller in a written contract. The scope of the contract must be elaborated in accordance with the European Commission's standard contractual clauses for data transfers. Nevertheless, the Office must authorise such a transfer. In contrast, the transfer of data to third countries in a controller-to-controller scenario does not require the Office's approval.

8.2.2 Binding corporate rules

There are no specific rules on binding corporate rules, but they are acknowledged as a legitimate ground for approving the transfer (Slovakia participates in the mutual recognition procedure, but from a legal point of view, formal authorisation is still needed).

8.2.3 Safe Harbour

There is no need for authorisation if the personal data are transferred to a US organisation that is certified under the US Safe Harbour scheme, unless it concerns a situation when the controller entrusts an entity residing abroad with the processing of the personal data on the controller's behalf, which must be authorised by the Office (ie, the approval of the Office is required

only in controller-processor scenarios, while controller-controller transfers may be conducted freely).

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The DPAct requires controllers and processors to ensure the security of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorised access, and making them available, as well as against any other unauthorised forms of processing.

9.2 Security requirements

Controllers and processors must take technical, organisational, and personal security measures adequate to the manner of processing, while taking into account, among other things, existing technical means; the extent of any possible risk that could violate the security or functionality of the filing system; confidentiality; and the importance of the processed personal data.

The abovementioned measures taken by the controller and processor must take the form of a security project of the filing system ('security project'):

(i) if special categories of personal data are processed, and the filing system is interconnected with a publicly accessible computer network, or if it is operated in a computer network interconnected with a publicly accessible computer network;
(ii) if special categories of personal data are processed (in such a case, the controller and the processor only need to document the technical, organisational, and personal measures taken); or
(iii) if the filing system is used for safeguarding the public interest.

A security project includes a security policy; analysis of the filing system's security; and security guidelines.

9.3 Data security breach notification obligation

Under Slovak law, there is no obligation to notify the data subjects and/or the Office of any personal data security breaches.

9.4 Data protection impact assessments and audits

Where a security project is to be developed, the analysis of the filing system's security forms part of the security project. It should be a detailed analysis of the state of the filing system's security, containing, above all:

- a qualitative risk analysis, where threats affecting individual items of the filing system that are capable of violating its security or functionality are identified;
- the result of the qualitative risk analysis is a list of threats that could endanger confidentiality, integrity, and availability of the processed personal data, while it also states the extent of the possible risk, proposals for the measures to eliminate or minimise the effect of the risk, and a list of the remaining risks;

- use of the security standards and determination of other methods and means of the protection of the personal data; and
- evaluation of conformity of the proposed security measures with the applied security standards, methods, and means.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Office may impose on controllers temporary obligations, remedial obligations in order to remove detected problems (eg, security project) or prohibit data processing, and order the liquidation of data. It may also publish information identifying controllers or processors who violated the DPAct.

The Office may carry out inspections, on its own initiative, or investigate any complaints it receives. It may carry out on-site investigations. In the course of an investigation, the controller must provide all the necessary information upon request and co-operate with the Office.

10.2 Sanctions

The processing of personal data in breach of the DPAct may constitute a criminal offence, penalised with imprisonment for up to two years.

The Office may impose on the controller or the processor a fine in the amount of €1,350 to €266,000 for a breach of the obligations ensuing from the DPAct. There may also be disciplinary fines of up to €53,000 for any failure to cooperate with the Office.

The Office does not publish statistics on the number of sanctions imposed. In our experience, currently data protection infringements rarely lead to the imposition of criminal penalties.

10.3 Examples of recent enforcement of data protection rules

In 2010, the Office imposed a penalty of €3,000 on a city office that installed fingerprint readers to monitor the attendance of its employees. Since the DPAct requires that such technology may be used only for securing access to specially protected objects or where high level of risk is present (such as nuclear power-plants), the use by the city office did not comply with these requirements.

Great controversy was caused by the national census in 2011 and the public dispute between the Office and Statistical Bureau on the nature of collecting personal data – the originally anonymous collection turned out not to be anonymous due to unique identifiers attached to the census forms. Nevertheless, the census was carried out and the Office is now investigating the matter further.

10.4 Judicial remedies

Data subjects are entitled to seek judicial protection. The DPAct stipulates that disputes arising from contractual or pre-contractual relations of controllers or processors and data subjects or other natural or legal persons, the hearing or deciding of which is subject to the respective courts or other

authorities pursuant to special acts, shall not be the subject of personal data protection supervision, ie the rights based on special acts are unaffected.

Provisions of the DPAct's section on rectification measures do not affect the right to judicial protection in administrative proceedings. The data subject can also seek redress under the general provisions on the protection of personal rights or claim damages on the basis of civil law provisions.

10.5 Class actions

Class actions are not permitted under Slovak law.

10.6 Liability

A person suffering any harm as a consequence of acts in breach of the provisions of the DPAct can initiate a civil action for damages. The controller and the processor are liable for damages resulting from an action in violation of the provisions of the DPAct. Data subjects that have incurred damage from an action in violation of the DPAct may thus claim damages from the controller and the processor.

South Africa

Adams & Adams André Visser & Danie Strachan

1. LEGISLATION

1.1 Name/title of the law

There is currently no dedicated legislation in South Africa that deals with data protection specifically.

Having said this, the protection of personal information is dealt with to an extent in provisions of legislation that deal with other topics. Those provisions are limited to the scope of the specific legislation in which they are found. The relevant statutes include the Consumer Protection Act, 2008 (CPA); the Electronic Communications and Transactions Act, 2002 (ECTA); the National Credit Act, 2005 (NCA); and the Promotion of Access to Information Act, 2000 (PAIA).

The right to privacy is provided for in section 14 of the Constitution of the Republic of South Africa.

1.2 Pending legislation

The Protection of Personal Information Bill, 2009 (POPI) was tabled in the South African parliament in 2009. Being a bill, POPI does not yet have the force of law. It is likely that changes will be made to the bill before it is finalised and is promulgated as an act. There is currently no indication of when POPI will come into force.

The purpose of POPI is to give effect to the constitutional right to privacy by providing for the safeguarding of personal information when being processed by a responsible party. Since South Africa has not had such legislation in the past, POPI will introduce a significant change in the country's legislation.

In the current absence of specific legislation, the provisions of POPI will be discussed in this chapter. As such, unless reference is made to other specific legislation, the principles discussed here are found in POPI. It must be kept in mind that the discussions are based on the version of POPI as it was available at the time of writing this chapter. Readers of this chapter should therefore check whether amended versions of the bill have become available, or whether POPI has subsequently come into effect in its current or amended form.

The Protection of Information Bill, 2010 (PIB), was tabled in the South African parliament during 2010 and should also be mentioned. Its purpose is to create a statutory framework for the protection of state information. This is information which is generated by state organs or which is in the possession or control of state organs. PIB sets out criteria and processes by which state information may be protected from destruction or from

unlawful disclosure, as well as procedures and criteria under which information may be classified.

1.3 Scope of the law

1.3.1 The main players

The main players found in POPI are as follows:

- the 'data subject' is 'the person to whom personal information relates';
- the 'responsible party' is 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'. A public body includes a natural person who carries on trade as well as a partnership and juristic (legal) person (excluding a public body). Public bodies include departments of state;
- the 'information protection officer'. In relation to a public body, the information protection officer will be the information officer or deputy information officer as contemplated under sections 1 or 17 of PAIA. In respect of a private body, this would be the head of a private body as contemplated in section 1 of PAIA;
- the 'operator' is 'a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party'; and
- the 'information protection regulator' (the Regulator) which will have various powers and duties under POPI.

1.3.2 Types of data

'Personal information' is defined in POPI as '*information relating to an identifiable, living, natural person, and where it is applicable, an identifiable existing juristic person, including, but not limited to:*

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number or other particular assigned of the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- *the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.*'

1.3.3 Types of acts/operations

POPI covers the processing of personal information entered into a record by or for a responsible party. POPI defines 'processing' as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as blocking, degradation, erasure or destruction of information.

1.3.4 Exceptions

POPI does not apply to processing of personal information:

- in the course of purely personal or household activity;
- where personal information has been de-indentified to the extent that it cannot be re-identified again;
- the processing of information by or on behalf of the state, if it involves national security, defence or public safety; or the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information;
- processing exclusively for journalistic purposes where the responsible parties, by virtue of their office, employment, or profession are subject to a code of ethics that provides for the protection of personal information;
- the processing of personal information by cabinet and its committees, the executive council of a province and a municipal council of a municipality;
- the processing of information relating to the judicial functions of a court; or
- where the processing of personal information has been exempted by the Regulator.

1.3.5 Geographical scope of application

POPI applies to the processing of personal information by or for a responsible party domiciled in South Africa.

If the responsible party is not domiciled in South Africa, POPI would apply if the processing uses automated or non-automated means situated in South Africa, unless those means are used only for forwarding personal information. Where information is processed by non-automated means, it must from part of a filing system or be intended to form part of it in order for POPI to apply. A filing system is defined as 'any structured set of personal information which is accessible according to specific criteria'.

1.3.6 Particularities

POPI regulates personal information of natural persons as well as of

identifiable, existing juristic persons. POPI also prohibits the processing of 'special personal information', unless specifically permitted by it.

ECTA contains data protection principles that can be subscribed to if personal information is collected during an electronic transaction. Subscription to the principles is voluntary, but if a data controller chooses to subscribe to them, it must subscribe to all of the principles. (A 'data controller' is defined as 'any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject'.) The principles are as follows:

- A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
- A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
- The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
- The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
- The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
- A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.
- The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
- The data controller must delete or destroy all personal information which has become obsolete.

A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

2. DATA PROTECTION AUTHORITY

The Regulator will only be established when POPI enters into force.

2.1 Role and tasks

The Regulator must promote an understanding and acceptance of the information protection principles contained in POPI. It is required to

undertake educational programmes and to make public statements on information protection. It must also undertake research into and keep itself abreast of information processing and computer technology in order to ensure that the adverse effects of such developments on the protection of the personal information of data subjects are minimised.

A number of the Regulator's duties pertain to its relationship with the South African Parliament. For instance, it has the duty to examine any proposed legislation that may have an effect on the protection of personal information. Further, it must report to parliament on any matter that may affect the protection of the personal information of a data subject. This may include any requirements for legislative, administrative or other action to improve the protection of personal information.

The Regulator is required to maintain registers of information processing, as required by POPI. The registers must be published and made available in accordance with POPI's provisions.

The Regulator is obliged to receive and investigate complaints concerning alleged violations of the protection of personal information of data subjects. In addition, it is tasked with conducting investigations under POPI's provisions and enforcing compliance. POPI lists various dispute resolution powers and duties of the Regulator.

2.2 Powers

The powers of the Regulator are interlinked with its duties (see section above).

2.3 Priorities

Since the Regulator has not yet been established, no priorities have been set.

3. LEGAL BASIS FOR DATA PROCESSING

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

Personal information may only be processed if:

- the data subject consents to the processing;
- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

The personal information of a data subject may not continue to be processed if a data subject has objected to it.

POPI regulates the processing of 'special personal information'. Unless specifically permitted, a responsible party may not process personal information concerning:

- a child who is subject to parental control; or
- a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.

The exemption on processing of special personal information does not apply where such processing is carried out with prior parental consent, if the data subject is a child and is subject to parental control under the law. The prohibition also does not apply if the processing is necessary to establish, exercise or defend a right or obligation in law, where processing is necessary to comply with an obligation of international public law, where the Regulator has granted such permission or the processing is carried out with the consent of the data subject or the information has deliberately been made public by the data subject.

Information regarding a data subject's religious and philosophical beliefs is permitted if done by spiritual or religious organisations in respect of data subjects belonging to such organisations or institutions founded on religious or philosophical principles with respect to their members or employees.

Information concerning race may be processed for the purposes of identifying the data subject or for the purposes of advancing laws or measures designed to protect or advance persons or categories of persons disadvantaged by unfair discrimination.

The exemption on processing information concerning trade union membership does not apply if the processing is done by the trade union to which the data subject is a member for the purpose of furthering the aims of the union.

Information on the political persuasion of a data subject may be performed if the processing is performed by an institution founded on political principles with regard to their members.

The exemption on processing of personal information concerning the health or sexual life of a data subject does not apply if performed by medical professionals and health institutions or social services for the purposes of treatment and care of the data subject. It may also be processed by insurance companies, medical aid schemes and managed healthcare organisations for the purposes of assessing risk, the performance of an insurance or medical aid agreement or the enforcement of any contractual rights and obligations. Such information may also be processed by schools to provide support to pupils, as well as by institutions of probation, child protection or guardianship for the performance of legal duties. Exemptions from the processing of such information are also provided in favour of certain government ministers and, in certain circumstances, to administrative bodies, pension funds, employers or institutions working for them.

The processing of information pertaining to the criminal behaviour of a data subject does not apply where such information is obtained for the purposes of fulfilling the ends of justice or is processed by responsible parties who have obtained such information lawfully.

3.1 Consent

3.1.1 Definition

'Consent' means '*any voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to him or her*'.

3.1.2 Form

No specific form is prescribed.

3.1.3 In an employment relationship

Since POPI will also apply in an employment relationship, consent would constitute a valid legal basis for data processing in that context

3.2 Other legal grounds for data processing

Personal information may also be processed where:

- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

3.3 Direct marketing and cookies

Under POPI, the processing of personal information of a data subject for the purpose of direct marketing by means of automatic calling machines, facsimile, SMS or electronic mails is prohibited unless the data subject consents to such processing or the data subject is a customer of the responsible party.

Where the data subject is a customer of the responsible party, the personal information of the data subject may still only be processed in specific circumstances, such where the responsible party obtained such contact details of the data subject in the context of a sale of products or services; or the purpose of the direct marketing of the responsible party is the marketing of the responsible party's own similar products or services.

Any communication initiated for the purposes of direct marketing must contain details of the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send a request that such communication cease.

The CPA regulates direct marketing in particular and provides consumers with the right to restrict unwanted direct marketing. This right includes the right to refuse to accept, to require another person to discontinue or to pre-emptively block any communication the purpose of which is direct marketing. A consumer may thus require any person who approaches it

for purposes of direct marketing, within a reasonable time to desist from initiating any further communication. The section also makes provision for the establishment of a registry in which consumers may register a pre-emptive block either generally or for specific purposes. The registry for pre-emptive blocking purposes is currently being established and the provisions relating to pre-emptive blocking are not yet in force. Consumers may rescind transactions that arise from direct marketing within a specified time period.

ECTA also deals with unsolicited commercial communications. In particular, the communication must provide the recipient with the option to stop subscription to a mailing list. At the recipient's request, the sender must also provide the recipient with identifying particulars of the source from which the sender obtained the recipient's personal information.

ECTA does not contain any provisions that relate specifically to the use of cookies.

3.4 Data quality requirements

Personal information may only be processed if it is adequate, relevant and not excessive, having regard to the purpose for which it was obtained.

The responsible party must take reasonably practicable steps to ensure that the personal information processed by it is complete, accurate, not misleading and updated where necessary. The responsible party must always have regard to the reason for which the information was collected or further processed.

The further processing of personal information must be compatible with the purpose for which it was collected initially. The following factors must be considered in this regard:

- the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
- the nature of the information concerned;
- the consequences of the intended further processing for the data subject;
- the manner in which the information was collected; and
- any contractual rights and obligations between the parties.

3.5 Outsourcing

An operator or anyone processing personal information on behalf of a responsible party must process such information only with the knowledge or authorisation of the responsible party. They must treat personal information which comes to their knowledge as confidential and must not disclose it unless required to do so by law or in the course of the proper performance of duties.

The processing of personal information for a responsible party by an operator on behalf of the responsible party must be governed by a written contract between the operator and the responsible party. The contract must require the operator to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

Where the operator is not domiciled in the Republic of South Africa, the responsible party must take reasonable steps to ensure that the operator

complies with the laws, if any, relating to the protection of personal information of the territory in which the operator is domiciled.

3.6 Email, internet and video monitoring

3.6.1 General rules

POPI does not contain any specific rules on email, internet and video monitoring. The interception of communications is governed by the Regulation of Interception of Communications and Provisions of Communication-Related Information Act, 2002 (RICA).

'Intercept' means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device so as to make some or all of the contents of communication available to another person other than the sender and recipient or intended recipient. This includes the monitoring of such communication using a monitoring device; viewing, examination or inspection of the contents of any indirect communication, the diversion of any indirect communication from its intended designation to any other destination.

Direct communication means aural communication which occurs between two or more people in the presence of all the people participating in such communication. It includes utterances which may be made in relation to indirect communication if the utterances made are audible to another person who is in the same room as the person partaking in indirect communication.

Indirect communication means the transfer of information, including a message or any part of a message, whether a speech, music or other sound, data, text, visual images (animated or not), signals or radio frequency spectrum, or any other form or combination of forms that is transmitted in whole or in part by means of a postal service or a telecommunication system.

As a general rule, communications may not be intercepted within South Africa, but there are exceptions. The specific circumstances in which communications may be intercepted can be summarised as follows:

- where a person or a law enforcement officer is a party to the conversation and does not intercept for the purposes of committing an offence or the law enforcement officer has obtained an interception direction;
- the person intercepting has received prior written consent from one of the parties to intercept the communication;
- indirect communication may be intercepted in the course of its transmission over a telecommunication system if the interception takes place in the course of the carrying on of any business and a transaction is entered into through that communication in the course of that business, or the communication otherwise relates to the business or otherwise takes place in the course of the carrying on of that business;
- interception of communication to prevent serious bodily harm; and
- interception of communication for purposes of determining location in cases of emergency.

Telecommunication service providers are required, under section 30 of

RICA, to provide a telecommunications service that is both capable of being intercepted and capable of storing information. RICA also regulates to whom real-time or archived communication-related information can be provided and under what circumstances.

3.6.2 Employment relationship

POPI does not deal with the monitoring of communications specifically, but it would still apply generally to an employment relationship in conjunction with RICA.

4. INFORMATION OBLIGATIONS

4.1 Who

A responsible party may only process personal information if it has taken reasonably practicable steps to inform the data subject.

4.2 What

The responsible party must take reasonably practicable steps to ensure that the data subject is aware of:

- the information being collected;
- the name and address of the responsible party;
- the purpose for which the information is being collected;
- whether or not the supply of the information by that data subject is voluntary or mandatory;
- the consequences of failure to provide the information;
- any particular law authorising or requiring the collection of the information; and
- any further information, such as the recipient or category of recipients of the information, the nature or category of the information and the right of access to and the right to rectify information collected.

4.3 Exceptions

A responsible party that has previously notified a data subject of its processing of information will comply with POPI's requirements regarding subsequent collection from a data subject if such collection relates to the same information or information of the same kind is collected and if the purpose of collection of the information is unchanged.

Further, a responsible party does not have to notify a data subject if:

- the data subject has provided consent for non-compliance;
- non-compliance does not prejudice the legitimate interest of the data subject as set out in POPI;
- non-compliance is necessary to avoid prejudice to the maintenance of the law; the enforcement of the law imposing a pecuniary penalty; the enforcement of legislation concerning the collection of revenue; for the conduct of proceedings in any court or tribunal; or the interest of national security;
- compliance will prejudice the lawful purpose of the collection;
- compliance is not reasonably practicable in the circumstances of the

particular case; or
- the information will not be in a form in which the data subject may be identified or it will be used for historical, statistical or research purposes.

4.4 When
If personal information is collected directly from a data subject, the data subject must be made aware before the information is collected, unless the data subject is already aware of the information that needs to be brought to the data subject's attention. In any other case, notification must take place before the information is collected or as soon as reasonably practicable after it has been collected.

4.5 How
No manner of form is prescribed, but the responsible party must take reasonably practicable steps to ensure that the data subject is aware of the matters mentioned in POPI in this regard.

5. RIGHTS OF INDIVIDUALS
5.1 Access
5.1.1 Right
Data subjects who have identified themselves properly have the right to request a responsible party to confirm, free of charge whether or not the responsible party holds personal information about the data subject and to request a description of the personal information about the data subject.

By virtue of the provisions of the NCA, every person has the right to be advised by a credit provider if adverse credit information concerning that person will be reported to a credit bureau. Such a person is entitled to receive a copy of the information. Every person may inspect any credit bureau, or national credit register, file or information which concerns that person without charge. A person may change the accuracy of information held by a bureau and concerning such person.

PAIA also facilitates access to records held by public or private bodies for the purposes of protecting or enforcing personal rights. This right has to be balanced with the need to protect private information. As such, a public or private body must provide a record, including one containing personal information, to a requestor or a person acting on behalf of a requestor if such information is required for the purposes of exercising or protecting a personal right.

5.1.2 Exceptions
Access may or must be refused if there are grounds for refusal attaching to such information as set out in PAIA. Every other part which may not be refused must be disclosed to the applicant.

Under PAIA, the right to access can be refused for the purposes of reasonable protection of privacy, commercial confidentiality as well as effective, efficient and good governance.

Further, in the absence of the requisite consent, the right to access may be

refused where:

- the information sought entails the disclosure of private information of a third party who is a natural person;
- where the information is part of certain records of the South African Revenue Services;
- where disclosure will amount to a breach of confidence owed to a third party;
- where disclosure will prejudice the protection of the safety of individuals and the protection of property or the defence, security and international relations of the Republic of South Africa;
- documents are privileged from production in legal proceedings;
- disclosure would be likely to materially jeopardise the economic interests or financial welfare of the Republic of South Africa or the ability of government to manage its economy effectively and in the country's best interest;
- the information pertains to research being done by or on behalf of a third party or the operations of a public body; or
- if the request is manifestly frivolous and vexatious or the request will substantially and unreasonably divert resources of the public body.

5.1.3 Deadline

A description of the personal information must be provided within a reasonable time after the relevant request.

5.1.4 Charges

Where a fee is payable in order to obtain information held by a responsible party, the responsible person must give the data subject an estimate of the fee. The information will only be given if it does not fall under information to which the grounds for refusal apply.

5.2 Rectification

5.2.1 Right

The data subject may request the responsible party to correct personal information about the data subject in its possession or under its control if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.

If a responsible party has taken steps to change information and such changes have an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of such steps. A responsible party must also notify a data subject where his request to make a correction is successful, and any action taken as a result of such request.

5.2.2 Exceptions

No specific exceptions are provided, but if agreement cannot be reached between the responsible party and the data subject, the responsible party

can take such steps as are reasonable in the circumstances, to attach to the information an indication that a correction has been requested but not made.

5.2.3 Deadline
Steps must be taken on receipt of a request for correction.

5.2.4 Charges
POPI does not deal with correction charges.

5.3 Erasure
5.3.1 Right
A data subject may request a responsible party to delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or if the responsible party is no longer authorised to retain it under the provisions of POPI.

5.3.2 Exceptions
See section 5.2.2 above.

5.3.3 Deadline
See section 5.2.3 above.

5.3.4 Charges
See section 5.2.4 above.

5.4 Blocking
5.4.1 Right
POPI does not deal with the blocking of personal information by data subjects, but see the comments under section 5.2 above.

5.4.2 Exceptions
Not applicable.

5.4.3 Deadline
Not applicable.

5.4.4 Charges
Not applicable.

5.5 Objection
5.5.1 Right
POPI does not deal with the objection to personal information held by responsible parties, but please see the comments under sections 5.2 and 3.3 above.

5.5.2 Exceptions
Not applicable.

5.5.3 Deadline
Not applicable.

5.5.4 Charges
Not applicable.

5.6 Automated individual decisions
5.6.1 Right
No one may be subject to a decision to which are attached legal consequences or which affects him to a substantial degree, if the decision has been taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his personality or personal habits.

5.6.2 Exceptions
Automated decision making is permitted if taken in connection with the conclusion or execution of a contract and the request of the data subject under the contract has been met or appropriate measures have been taken to protect his legitimate interests. The automated decision making may also take place if the decision is governed by a law or code in which appropriate measure are specified for protecting the legitimate interests of data subjects.

5.6.3 Deadline
Not provided for.

5.6.4 Charges
Not provided for.

5.7 Other rights
5.7.1 Right
A data subject who is a subscriber to a printed or electronic directory of subscribers available in which his personal information is included must be informed free of charge and before the information is included in the directory of the purpose of the directory and any further uses to which the directory may possibly be put. The data subject must be afforded a reasonable opportunity to object to such use or request verification, confirmation or withdrawal.

6. REGISTRATION OBLIGATIONS
6.1 Notification requirements
6.1.1 Who
Personal information may only be processed by a responsible party if the Regulator has been notified.

6.1.2 What
A responsible party must notify the Regulator before the start of fully or partly automated processing of personal information or categories of

personal information intended to serve a single purpose or different related purposes. It must also notify the regulator if it conducts non-automated processing of personal information intended to serve a single purpose or different related purposes, if this is subject to a prior investigation (see section 6.3 below).

6.1.3 Exceptions

The Regulator may exempt the processing of certain categories of information which do not have the effect of infringing the legitimate interests of a data subject.

A responsible party that has compiled and made available a manual under PAIA, does not have to notify the Regulator that it is processing personal information, if the particulars referred to in POPI are contained in the manual.

6.1.4 When

The notification must be made before the start of the processing of the information.

6.1.5 How

The notification must contain the following information:

- the name and address of the responsible party;
- the purpose of processing;
- description of the categories of data subjects and of the information or the categories of information relating thereto;
- the recipient or categories of recipients to whom the information will be supplied;
- planned trans-border flows of personal information; and
- a general description allowing a preliminary assessment of suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

A responsible party need only give notice once and not every time personal information is received or processed. POPI also regulates the notification of any changes to particulars in an initial notification.

6.1.6 Notification fees

No fees have been prescribed yet.

6.2 Authorisation requirements

6.2.1 Who

A responsible party may be authorised by the Regulator to process personal information, even if that processing is in breach of an information protection principle.

6.2.2 What

The Regulator may authorise the processing of personal information, even if the processing will breach an information protection principle, if:

- public interest in the processing outweighs interference to a substantial degree; or
- processing involves a clear benefit to the data subject or a third party that outweighs interference to a substantial degree.

6.2.3 Exceptions
Not applicable.

6.2.4 When
Not applicable.

6.2.5 How
Not applicable.

6.2.6 Authorisation fees
Not applicable.

6.3 Other registration requirements
The Regulator must initiate an investigation prior to any processing if the responsible party plans to process the following information:

- a number identifying data subjects for a purpose other than the one for which the number is specifically intended, with the aim of linking the information together with information processed by other responsible parties, unless authorised by the Regulator;
- information on criminal behaviour or on unlawful or objectionable conduct on behalf of a third party;
- for the purposes of credit reporting.

Prior investigation must also take place if the responsible party plans to transfer special personal information to foreign countries without adequate information protection laws.

A responsible party must notify the Regulator of the processing of the information mentioned in this section 6.3. The Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation. The Regulator must indicate the period within which it plans to conduct such an investigation. On conclusion of the investigation, the Regulator must issue a statement concerning the lawfulness of the information processing. If the responsible party does not receive the Regulator's decisions within the prescribed time limits, it may presume a decision in its favour.

6.4 Register
The Regulator must maintain an up to date register of the information processing notified to it. The register must at least contain the information provided in a responsible party's notification of processing. Such information must include the name and address of the responsible party; the purpose of the processing; a description of the categories of data subject and information; the recipients or categories of recipients to whom the personal

information may be supplied; planned trans-border flows of personal information and a general description allowing a preliminary assessment of the suitability of the information security measure to be implemented by the responsible party.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

POPI recognises the role of an information protection officer and deputy information officers. Information protection officers may only perform their functions once registered by the responsible party with the Regulator.

7.2 Tasks and powers

The information protection officer has the responsibility to:

- encourage compliance by the designating body with the information protection principles;
- deal with requests made to the designating body;
- co-operate with the Regulator in instances of investigations; and
- ensure compliance with the law governing the protection of personal information.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

A responsible party many not transfer personal information to a third party in a foreign country unless:

- the recipient of such data is subject to a law, a binding code of conduct or a contract which upholds the principles for reasonable processing of information in a similar fashion to the information principles as set out in POPI;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion of a contract in the interest of the data subject between the responsible party and the third party; or
- the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to the transfer and, if such consent could be obtained, the data subject would most likely give it.

8.2 Legal basis for international data transfers

8.2.1 Data transfer agreements

Not specifically provided for.

8.2.2 Binding corporate rules

Not specifically provided for.

8.2.3 Safe Harbour

Not specifically provided for.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate reasonable technical and organisational measures to prevent any loss, or unauthorised destruction of personal information and unlawful access to or processing of personal information.

9.2 Security requirements

The responsible party must take reasonable measures to:

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are efficiently implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

A responsible party and operator must have regard to generally accepted information security practices and procedures which apply to it or may apply to it in respect of specific industry or professional rules and regulations.

9.3 Data security breach notification obligation

9.3.1 Who

A data security breach must be notified by the responsible party or a third party processing personal information under the authority of a responsible party.

9.3.2 What

Notification must take place if there are reasonable grounds to believe that personal information of a data subject has been accessed or acquired by any unauthorised person.

9.3.3 To whom

The Regulator as well as the data subject (unless the identity of such data subject cannot be established) must be notified.

9.3.4 When

The notification must be made as soon as reasonably possible after it is discovered that there has been a compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. The responsible party may only delay notification to the data subject if the South African Police Services, the National Intelligence Agency or the Regulator directs that notification will impede a criminal investigation.

9.3.5 How

The notification sent to the data subject must be in writing and must be communicated either by mail to the data subject's last known physical or postal address, by email to their last known email address, by placing the notice in a prominent position on the responsible party's website, by publication in the news or in a manner directed by the Regulator.

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise. It must include the identity of the unauthorised person who accessed or acquired the personal information, if this is known.

9.3.6 Sanctions for non-compliance

Currently, no sanction has been prescribed for non-compliance.

9.4 Data protection impact assessments and audits

This is not provided for under South African law.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

A person may submit a complaint to the Regulator, if he alleges that there has been interference with his personal information. The Regulator may then decide to commence an investigation. It may also act as a conciliator and take any further action, as it may be empowered to take. The Regulator can also investigate matters of its own accord.

If the Regulator is satisfied that there has been interference with the protection of personal information of a data subject, the Regulator may serve an enforcement notice on the responsible party. The Regulator may require the responsible party to take specified steps to refrain from the interference or to stop the processing of personal information.

10.2 Sanctions

The following actions constitute offences under POPI:

- obstruction of the Regulator;
- breach of POPI's confidentiality provisions;
- obstruction of the execution of a warrant; and
- failure to comply with enforcement or information notices.

Any person convicted of an offence under POPI can be sanctioned with a fine and/or imprisonment. In a case where the offender has hindered, obstructed or unlawfully influenced the Regulator, the term of imprisonment may not exceed 10 years. In any other case, the imprisonment period may not exceed 12 months.

10.3 Examples of recent enforcement of data protection rules

Since POPI is not yet in force, there are no examples of enforcement.

10.4 Judicial remedies

Contraventions of POPI can be tried in South African courts. POPI

specifically states that magistrate's courts have jurisdiction to impose penalties in respect of contraventions.

10.5 Class actions

POPI does not make provisions for class actions.

10.6 Liability

A data subject or, at the request of the data subject, the Regulator may institute civil action for damages in a court against the responsible party for interference with the protection of the personal information. This may be done whether or not there is intent or negligence on the part of the responsible party. A court hearing such proceedings may award an amount that is just and equitable, which may include payment of damages, aggravated damages, interest and costs of suit.

Spain

Uría Menéndez
Cecilia Álvarez Rigaudias & Leticia López-Lapuente

1. LEGISLATION

1.1 Name/title of the law

The Spanish legal framework for the protection of personal data is regulated by: (i) the Lisbon Treaty; (ii) Article 18(4) of the Spanish constitution; and (iii) Law 15/1999 on the protection of personal data (the DP Act), as developed by Royal Decree 1720/2007. The provisions of the DP Act are mandatory and, consequently, parties to an agreement falling under its scope are not entitled to waive its application.

The Spanish data protection supervisory authority (the DPA) has issued instructions aimed at developing the DP Act's general principles on specific processing activities including, for example, joint contracting of life insurance policies and loans, control of access to premises, video surveillance, etc.

The DPA also governs the application and enforcement of the provisions of other laws related to the processing of information which may (or may not) consist of 'personal data'. This is the case for specific provisions relating to cookies and direct marketing by email or other equivalent means of e-communications, fax and telephone without human intervention falling under the scope of the E-Commerce Act 34/2002 (the E-Commerce Act) and the General Telecommunications Act 32/2003 (the Telecommunications Act), developed by Royal-Decree 424/2005, which have transposed Directives 2000/31/EC and 2002/58/EC (ePrivacy Directive) into Spanish law. The provisions of the DP Act apply cumulatively to these rules when 'personal data' are processed.

1.2 Pending legislation

The current Spanish provisions on cookies and breaches of notification are in the process of being amended to implement Directive 2009/136/EC (see section 3.3 and 9.3).

1.3 Scope of the law

1.3.1 The main players

- The 'data controller' is a 'natural or legal person, whether public, private or an administrative body, which determines the purposes, content and use of the processing'.
- The 'data processor' is a 'natural or legal person, public authority, service or any other body that, individually or jointly with others, processes personal data on behalf of the controller'.

- The 'data subject' is an individual to whom the personal data being processed refer.
- The 'third party' is an individual or legal person, whether public, private, or an administrative body other than the data subject, the data controller, the data processor or the persons authorised to process the data under the direct authority of the data controller or data processor. Entities without legal personality acting as separate parties in the operation may also be considered as third parties.

1.3.2 Types of data

'Personal data' refers to any information relating to an identified or identifiable individual. Legal persons and irreversibly anonymous data are excluded from the scope of the DP Act.

The following categories of data are subject to reinforced protection: (i) ideology, trade union membership, religion and beliefs; (ii) racial origin, health and sexual life; and (iii) criminal or administrative offences.

1.3.3 Types of acts/operations

The DP Act covers the processing of data and databases. 'Processing' is defined as 'operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and cancellation, as well as assignments of data resulting from communications, consultations, interconnections and transfers'.

Database means 'any structured set of personal data, irrespective of the form or method of its creation, storage, organisation or access'.

1.3.4 Exceptions

The following databases fall outside the scope of the DP Act:

- those maintained by an individual in the course of a purely personal or household activity;
- those falling under the scope of regulations on official secrets; and
- those on terrorism and serious organised crime investigations (although the DP Act does not apply, the DPA must be previously informed of their existence).

1.3.5 Geographical scope of application

The DP Act is mainly applicable:

- if the processing is carried out by a permanent establishment in Spain of the data controller; or
- if a data controller established outside the EU makes use of equipment, whether or not automated (other than for transit purposes), located in Spain (in which case, the data controller must appoint a legal representative in Spain).

1.4 Particularities

The following processing of personal data is governed by specific provisions

and, to the extent no such provision exists, by the DP Act's special provisions:

- databases regulated by Spanish legislation on the electoral system;
- databases used for statistical purposes by Spain's central or regional governments;
- databases intended for the storage of data contained in personal assessment reports under the legislation of the Armed Forces Code;
- databases contained in the Civil Registry and Criminal Registry; and
- databases which store images and sounds recorded by the video cameras of the Armed Forces.

2. DATA PROTECTION AUTHORITY

The DPA's details are the following:
Agencia Española de Protección de Datos
Jorge Juan, 6 - CP 28001, Madrid, Spain.
T: +34 901 100 099
+34 91 266 35 17
E: ciudadano@agpd.es
W: www.agpd.es

In addition to the above, the following regional data protection authorities should also be considered on the basis that they hold limited jurisdiction on the processing by the public sector in their respective region:

Region	Madrid	Catalonia	Basque Country
Name	Data Protection Agency of the Madrid Autonomous Region	Catalonian Data Protection Authority	Basque Data Protection Agency
Address	C/ Cardenal Marcelo Espinola 14, 3º CP/28016 Madrid	C/ de la Llacuna 116, 7º CP/08018, Barcelona	C/ Beato Tomas Zumarraga 71 3º CP/ 01008 Gasteiz- Vitoria
Tel:	+34 91 580 28 74	+34 93 552 78 00	+34 945 016 230
Web:	*www.Madrid.org/apdcm*	*www.apdtcat.net*	*www.avpd.euskadi.net*

2.1. Role and tasks

The DPA is the independent authority responsible for the application of the DP Act. In particular, it has the power:

- to grant authorisations prescribed by the DP Act (eg, for international transfers, when required);
- to enact instructions in order to ensure that the processing of personal data is carried out in a manner consistent with the DP Act;
- to carry out investigations (including access to the data) and to collect all necessary information for the performance of its supervisory duties;
- to order the blocking, erasure or destruction of data, imposing temporary or definitive bans on processing, warning or reprimanding the data controller, or imposing fines for infringements under the DP Act, the E-commerce and the Telecommunications Acts;

- to provide the data subjects with information on their rights and to hear claims concerning personal data protection under the DP Act;
- to publish databases that are registered with the DPA's Registry (see section 6.4 below); and
- to publish annual reports of its main activities.

2.2. Priorities

One of the priorities of the DPA in recent years has been to increase citizens' awareness of their personal data protection rights, primarily by maintaining a constant and active presence in the media and by answering the increasing number of questions submitted to it by citizens and companies.

Furthermore, the DPA has paid special attention to the protection of individuals on the internet (particularly regarding minors and social networks and the 'right to be forgotten'), the protection of health-related data and the correct performance of the international transfer of personal data.

CCTV systems and telecommunications services are the two activities which have been subject to the highest number of sanctions in recent years, followed by the financial sector (in particular, the disclosure of debts in connection with creditworthiness and solvency files) and spamming activities.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

The processing of personal data requires the data subject's consent, unless the processing falls under the scope of one of the other legitimate grounds exhaustively listed in the DP Act (see sections 3.2 and 3.5 below). 'Data subject's consent' means any unambiguous, freely given, specific and informed indication of an intention by virtue of which the data subject signifies his agreement to the processing of his personal data.

The data subject's consent may be revoked if there exists a justified cause. The revocation of consent will not have retroactive effect.

3.1.2 Form

Consent may be explicit or tacit, unless the law expressly requires a specific form of consent. Explicit consent is required, for example, in connection with the processing of sensitive data or direct marketing activities sent by e-communications, automatic calls or fax.

3.1.3 In an employment relationship

As with all data processing, the processing of personal data for employment purposes requires the data subject's consent, unless the processing is based on a legal exception to that requirement. The most common exceptions are the following:

(i) only for non-sensitive data: the performance or control of the employment contract; and
(ii) for both non-sensitive data and sensitive data: compliance with (Spanish) legal obligations, such as social security, tax, work permits, etc.

The processing of employees' personal data must be adequate, relevant and not disproportionate in relation to the purposes for which the data are processed. This rule must be observed for any processing of personal data, but it is especially relevant if sensitive data are being processed for human resources purposes.

3.2 Other legal grounds for data processing

The processing of non-sensitive personal data by data controllers requires the data subject's consent, unless:

Ground	Internal processing	Disclosure to another data controller
Public sector only	they are collected for functions corresponding to public authorities within the scope of their powers	the recipients of the data are the Ombudsman, the Office of the Public Prosecutor, Judges or the Court of Accounts (or their regional equivalent), and the disclosure is needed for the exercise of their functions the transfers are made between public authorities and the processing has historical, statistical, or scientific purposes.
Contractual necessity	the processing is necessary for the performance of a contract (which will be) signed by the data subject	the processing arises from the free and legitimate recognition of a legal relationship that necessarily implies the processing of the data by third party databases.
Legal ground	the processing is necessary for compliance with a legal obligation imposed on the data controller	transfer authorised by law
Vital interest	the processing is necessary for the vital interest of the data subject	disclosure of health-related data that are necessary for resolving a medical emergency or for epidemiological research as established by law
Sources available to the public	the data are included in limited sources available to the public (eg telephone directories, lists of persons belonging to professional associations, official gazettes and the media -internet not included) and the purposes of the processing are for the legitimate interests of the data controller or the third party to whom the data are disclosed, except if overridden by the interests or fundamental rights and freedoms of the data subject	data collected from limited sources available to the public

The processing of sensitive data by data controllers requires the data subject's consent, unless:

- for data on ideology, trade union membership, religious or other beliefs, racial origin, health and sexual life: Spanish law so authorises;
- for data on criminal and administrative offences: Spanish law so authorises and the data are only processed by the public administration;
- for health-related data for the purposes of preventive medicine or diagnosis, the provision of medical care or treatment, or the management of healthcare services: provided that such data processing is carried out by a health professional subject to the duty of professional secrecy or by another person also subject to an equivalent obligation of secrecy; or
- for health-related data to safeguard the vital interests of the data subject or another person: if the data subject is physically or legally incapable of providing consent.

3.3 Direct marketing and cookies

Unless the data are gathered from limited sources available to the public, the DP Act establishes that direct marketing activities require the data subject's prior consent.

The consent must be explicit if the direct marketing is sent by e-communication means, by fax or through automated calling systems (irrespective of whether or not the data from these limited sources is available to the public).

However, in connection with e-direct marketing:

- Explicit consent is not required provided that: (i) a prior contractual relationship exists between the data subject and the company sending the communication; (ii) the recipient's data have been lawfully obtained; and (iii) the communication concerns products or services of the company itself that are similar to those initially contracted.
- Upon collection of the data, and in each e-commercial communication, the recipient must be informed of his right to object (free of charge) to the use of his data for marketing purposes as well as of the procedure for exercising such right.
- Each and every e-commercial communication must: (i) be clearly identified as such and include the name of the natural or legal person on behalf of which it is made; and (ii) include the word 'advertising' at the beginning of the communication.

The E-Commerce Act allows the use of devices for data storage and recovery purposes in the recipient's terminal (eg, 'cookies') if the (information society) service provider: (i) provides the recipient with clear and comprehensive information about the use and purposes of the devices; and (ii) offers the recipient the possibility of opting out of the data processing without charge and in any easy manner. The provisions do not prohibit technical data storage or access for the sole purpose of carrying out or facilitating the transfer of information over e-communication networks, or where strictly necessary to provide an information society service as

explicitly requested by the recipient.

On 27 May 2011, the Spanish government published draft legislation in order to transpose the provisions of Directive 2009/136/EC on cookies, among others, into Spanish law. If the draft bill is approved as proposed, the user's consent for the use of cookies will be required. Nevertheless, the manner in which the consent would have to be obtained is not entirely clear. In any event, any such obligations would be subject to further legislative developments.

3.4 Data quality requirements

Specific rules govern the 'quality' of the processed data:

- the data must be accurate, complete and current;
- the data controller may not retain the data any longer than necessary for the purposes for which they were obtained or recorded (unless for historical, statistical or scientific research purposes in accordance with specific legislation);
- personal data subject to processing may not be used for purposes incompatible with those for which they were collected;
- personal data must be stored in a way that permits the exercise of the right to access (unless legally cancelled).

3.5 Outsourcing

The DP Act requires that, if the processing is carried out by a data processor, the data controller must execute a written agreement with the data processor indicating the specific obligations (the 'processing agreement') and establishing:

- that the data processor shall only act upon the data controller's instructions;
- the security measures to be implemented by the data processor (see section 9.2 below);
- that the data can only be processed on behalf of the data controller, and solely for the purposes agreed;
- that the data processor may not transfer the personal data to other legal bodies or individuals, including for storage (there are specific rules for subcontracting); and
- that the data must be destroyed or returned to the data controller once the service is provided.

3.6 Email, internet and video monitoring

3.6.1 General rules

As a general rule, email and internet monitoring activities are subject to a data subject's prior consent. Nevertheless, exceptions to that rule may arise in two main scenarios: (i) judicial and police surveillance; and (ii) monitoring in the workplace. In all cases, these activities must be proportionate (ie suitable, necessary and appropriate).

Video monitoring is generally permitted provided that: (i) there is a legitimate ground for its use (eg, a store taking measures against theft);

(ii) the measure is proportionate; and (iii) individuals are duly informed beforehand. The specific rules on the processing of personal data arising from the use of CCTV systems are contained in the DPA's Instruction 1/2006, whereby signs containing information regarding the data controller's identity and where to exercise data protection rights must be visibly posted where cameras are located, and paper forms with the data protection information clause must be available upon the request of data subjects. Furthermore, the images must be erased on a monthly basis. Database registration with the DPA is only required if the images are recorded.

3.6.2 Employment relationship

From a strict data protection standpoint, such monitoring activities are permitted provided that the measure is proportionate and that comprehensive information has been previously provided to the employees (in addition to the specific data protection information indicated in section 4 below) on: (i) the permitted/prohibited uses of the company's tools (email, internet or any other work tools provided by the employer for the performance of the tasks entrusted to employees); and (ii) its monitoring (which must be limited to professional use).

4. INFORMATION OBLIGATIONS

In addition to the information obligations described subsequently corresponding to the implementation of Articles 10 and 11 of the Directive, there also exist specific information duties regarding security measures, which are described in section 9 below.

4.1 Who

The information obligations apply to data controllers.

4.2 What

If personal data are obtained directly from the data subject, the data controller must inform the data subject of:

(a) the existence of a database or an on-going personal data processing operation affecting him;
(b) the identity and address of the data controller and, if the obligation to appoint a representative applies, its representative in Spain;
(c) the processing purpose(s) (and, if that includes direct marketing purposes: the details corresponding to the sector to which the products and services to be promoted belong);
(d) the data recipients (and, if consent is required for disclosure to the recipients, the information at this stage must at least include the recipient's activity and the purpose of the transfer); and
(e) additional information (unless its content can be clearly inferred from the nature of the personal data requested or the circumstances under which they were obtained), specifically: (i) whether or not the data collection is required and the consequence of (not) providing them; and

(ii) the right to access, rectification, cancellation and objection;

(f) if data pertaining to the subject's ideology, religion or beliefs are collected, the data subject must also be informed of his right not to give consent to the processing.

If the personal data are not directly obtained from the data subject, the data controller must provide the data subject with the same information as that mentioned previously (except for e (i) above), as well as the content of the processing and the origin of the data. However, if the personal data are collected from sources available to the public and are intended to be used for marketing activities, each communication sent to the data subject must inform him of the origin of the data, the identity of the data controller and his rights as the data subject.

As a general rule, the data controller must inform the data subjects (at the latest by the time of the transfer) of the disclosure, their purpose, the nature of the data to be disclosed and the name and address of the recipient.

4.3 Exceptions

Unless a specific legal provision establishes otherwise, there are no exceptions to the information duty if the personal data are directly obtained from the data subject.

If the personal data are not directly obtained from the data subject, no information is required if: (i) it has been previously provided to the data subject; (ii) the processing is carried out under the scope of a legal provision or for statistical, historical or scientific research purposes, (iii) if, in the opinion of the DPA, the provision of the information involves a disproportionate effort in view of the number of data subjects, the age of the data and the potential compensatory measures; or (iv) the personal data are from limited sources available to the public and are intended to be used for advertising activities or market research (in which case, as previously indicated, each communication sent to the data subject must inform him of the origin of the data, the identity of the data controller and his rights as the data subject).

4.4 When

If personal data are obtained directly from the data subject, the data controller must provide the data subject with the legally prescribed information at the time of collection. If not obtained directly from the data subject, the information must be provided within three months of their recording.

In the event of disclosure of the data, the data controller must inform the data subjects prior to the first transfer.

4.5 How

The information must be provided to the data subjects in an explicit, specific and unambiguous manner.

If the personal data are collected through a questionnaire or any other written method, the prescribed information must be clearly legible.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The data subject is entitled to request and obtain information from the data controller in a clear, legible and recognisable manner (with no keys or codes) regarding:

- the personal data that are being processed (including data initially collected or resulting from any further processing operation, as the case may be);
- the precise uses and purposes of the processing; and
- the origin of the data (each source should be specified if the data are collected from multiple sources) and the disclosures or transfers carried out or which are expected to be carried out in respect of the same (indicating the recipients to whom the data are disclosed or to be disclosed).

Upon exercising the right, the data subject may choose to be given access by means of a screen display, a written copy sent by post, a facsimile, an email or other e-communication means, or by any other method that may be suitable considering the nature of the database and the processing carried out by the data controller.

If the data controller offers a specific system for the effective exercise of the right of access and the data subject demands that it be carried out by virtue of a costlier procedure that has similar effectiveness and guarantees as the procedure offered by the data controller, the costs will have to be borne by the data subject.

5.1.2 Exceptions

The right of access may be rejected when:

- the access request is made by a person other than the data subject or his duly evidenced legal representative;
- the access request application is incomplete (eg, no proof of identity);
- Spanish law specifically prohibits the data controller from replying to the access request; or
- the request is made before 12 months have elapsed as from the date of a prior request by the same person that has been properly answered, unless the data subject can prove a legitimate interest.

In any event, the data controller must inform the data subject of his right to submit a complaint to the DPA or, if appropriate, to the supervisory authorities of the corresponding autonomous region. The authority will then order the data controller to properly answer the request and if it fails to do so, penalty proceedings may start.

Even if the request cannot be accepted, the data controller must nevertheless inform the applicant of that circumstance within the prescribed time period.

5.1.3 Deadline

The data controller must reply to the request seeking the exercise of the right

to access within 30 days of its receipt) and provide effective access within 10 days of issuing its reply.

5.1.4 Charges

The data controller may not demand payment for the costs incurred in replying to the data subject's request to exercise his right to access.

5.2 Rectification

5.2.1 Right

The data subject is entitled to request the rectification of personal data which are inaccurate or incomplete.

5.2.2 Exceptions

The request must be rejected when:

- the request is made by a person other than the data subject or his duly evidenced legal representative;
- the request is incomplete (eg, lacks proof of identity or includes inaccurate data); or
- the law specifically prohibits the data controller from accepting the request.

Even if the request must be rejected, the data controller must inform the applicant of that circumstance within the prescribed time period.

5.2.3 Deadline

The data controller must reply to the request to rectify or cancel data within 10 days as of its receipt.

If the data controller has transferred the data which are to be rectified to third parties, it must inform those third parties in order that they may also rectify the data.

5.2.4 Charges

The data controller may not demand payment for the costs incurred in replying to the data subject's request to exercise his right to rectify.

5.3 Erasure

5.3.1 Right

The data subject is entitled to request the cancellation of any personal data which are inappropriate or excessive, notwithstanding the blocking obligation described subsequently.

5.3.2 Exceptions

The request must be rejected when:

- submitted by a person other than the data subject or his duly evidenced legal representative;
- it is incomplete (eg, lacking proof of identity or includes inaccurate data); or
- the law specifically prohibits the data controller from accepting the

request.

Furthermore, the request to cancel data may be rejected if the cancellation could prejudice the legitimate interests of the data subject or of a third party, or if the data controller is under a legal obligation to maintain the data.

Even if the request must be rejected, the data controller must inform the applicant of that circumstance within the prescribed time period.

5.3.3 Deadline

The data controller must reply to the request to cancel data within 10 days of its receipt.

If the data controller has transferred the data to be cancelled to third parties, it must inform those third parties in order that they may also cancel that data accordingly.

5.3.4 Charges

The data controller may not demand payment for the costs incurred in replying to the data subject's request to exercise his right to cancellation.

5.4 Blocking

5.4.1 Right

Blocking is not a right as such but the legal (and automatic) consequence of the cancellation of data. It consists of identifying and retaining the data in order to prevent further active processing.

5.4.2 Exceptions

Blocked data must remain at the disposal of the public authorities for the purpose of determining any liability that may arise from the data controller or the data processor's processing. The obligation to maintain the blocked data will end upon the expiry of the liability and, then, the data must be deleted.

5.4.3 Deadline

The data controller must block the data at the time of the cancellation.

5.4.4 Charges

The data controller may not demand payment for the costs incurred in blocking the data.

5.5 Objection

5.5.1 Right

The data subject is entitled to object to the processing of his data when the processing:

- does not require his consent but the objection is justified based on a legitimate interest (and the law does not establish otherwise); or
- is carried out for direct marketing purposes.

5.5.2 Exceptions

The request must be rejected when:

- made by a person other than the data subject or his duly evidenced legal representative;
- it is incomplete (eg, lacking proof of identity or includes inaccurate data); or
- the law specifically prohibits the data controller from accepting the request.

Even if the request must be rejected, the data controller must inform the applicant of that circumstance within the prescribed time period.

5.5.3 Deadline

The data controller must reply to the request to object to the data within 10 days of its receipt.

5.5.4 Charges

The data controller may not demand payment for the costs incurred in replying to the data subject's application to exercise his right to object.

5.6 Automated individual decisions

5.6.1 Right

The data subject may challenge administrative acts and private decisions which involve an assessment of his behaviour, which is solely based on the automated processing of personal data which provides a definition of his characteristics or personality. In such event, the data subject will have the right to obtain information from the data controller on the assessment criteria and program used in the processing on the basis of which the decision of the act was adopted.

5.6.2 Exceptions

Data subjects may be subject to automated individual decisions which:

- are made within the framework of the execution or implementation of a contract at the request of the data subject, whenever he is afforded the possibility of providing arguments that he may deem to be relevant, for the purpose of defending his right or interest (in any case, the data controller must previously inform the data subject, clearly and precisely, that decisions will be made on the basis of his characteristics and that it will cancel the data in the event the contract is ultimately not executed); or
- are authorised by a rule of law that establishes measures that guarantee the data subject's legitimate interests.

5.6.3 Deadline

The data controller must reply to a challenge of an automated decision within 10 days of its receipt.

5.6.4 Charges

The data controller may not demand payment for the costs incurred in

replying to the data subject's request to exercise his right to challenge automated decisions.

5.7 Other rights

5.7.1 Right

At any time, any person may consult the DPA's Registry in order to determine whether his personal data are being processed, the processing purposes and the identity of the data controllers.

5.7.2 Exceptions

Not applicable.

5.7.3 Deadline

Not applicable.

5.7.4 Charges

Consulting the DPA's Registry is free of charge and is available to the public.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The data controller must comply with notification requirements.

6.1.2 What

The creation, modification and cancellation of any database containing personal data must be notified.

6.1.3 Exceptions

Excluding the processing/databases falling outside the scope of the DP Act (see section 1.3.4 above), there are no exemptions to the notification obligation.

6.1.4 When

- Creation of a database: the notification must be made prior to starting any processing.
- Updating a database: each time any of the notified fields requires modification.
- Suppression of a database: when the data have been erased.

6.1.5 How

The notification must be submitted to the DPA using the official form available on the DP Act's website (*www.agpd.es*) in Spanish. The data controller may be required by the DPA to correct any inaccuracy or mistake in the notification or provide more information. Otherwise, the DPA must register the database within 30 days from the application's filing date and assign the database a unique registration number to be used for further updates. If no answer is received from the DPA upon the expiry of that term,

the database will be considered as having been registered.

The notification procedure is different for databases controlled by public authorities. The creation, modification and cancellation of any database maintained by a public authority must be published in the Spanish Official Gazette (Boletín Oficial del Estado) or in the corresponding official gazette.

As per the last report published in August 2011, the DPA has received 439,740 notifications in 2011, out of which 361,355 regarding the creation, 46,668 the updating and 31,717 the suppression of a database. In 2010, the DPA received 623,148 database notification, out of which 527,919 regarding the creation, 64,429 regarding the updating and 30,800 the suppression of a database.

6.1.6 Notification fees

The notification is free of charge.

6.2 Authorisation requirements

6.2.1 Who

The data controller is responsible for requesting the DPA's authorisation.

6.2.2 What

The data controller must be granted the DPA's prior authorisation when the data are to be transferred to a country outside the EEA, unless the transfer falls under the scope of a legitimate ground (see section 8.2 below).

6.2.3 Exceptions

Prior authorisation from the DPA is not required for transferring personal data from Spain to a non-EEA country under the circumstances explained in section 8.2.

6.2.4 When

Prior to transferring the personal data to a 'non-adequate' recipient.

The procedure lasts for three months. The authorisation will be considered as having been granted if the DPA has not approved (or notified) an express resolution upon the expiry of that term. Once the authorisation is granted, it will be automatically registered with the Spanish DPA's Registry in the databases to which the transfer corresponds.

6.2.5 How

The request for authorisation must be submitted in Spanish to the DPA, and must at least contain:

- the databases containing the data on international transfers, indicating the name and registration code of the database in the DPA's Registry;
- the transfer/s for which the authorisation is being requested, indicating its/their purpose/s;
- the documentation on the prescribed guarantees for obtaining authorisation as well as the necessary compliance with law for the transfer, when required.

When the authorisation is based on the existence of a contract between the data exporter and the data importer, a copy of the contract and evidence of parties' sufficient legal powers must be provided.

If the authorisation is based on the binding corporate rules (BCRs), the BCRs must be provided as well as documentation that evidences that they are binding and effective within the group.

6.2.6 Authorisation fees

The authorisation request is free of charge.

6.3 Other registration requirements

Not applicable.

6.4 Register

Databases notified to the DPA are registered with the DPA's Registry and may be consulted for free on the DPA's website.

The following information is made public: (i) details on the controller; (ii) place where the data subject may exercise his rights of access, rectification, cancellation or objection; (iii) name and processing purposes; (iv) data sources and categories of data subjects; (v) categories of personal data and data processing system (automated or not); (vi) categories of recipients; and (vii) transfers outside the European Economic Area (EEA).

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The appointment of a Data Protection Officer (DPO) is limited to monitoring compliance with security requirements, and only when specific personal data are processed.

No specific legal rules apply to appointments. The appointment must only ensure that the data controller or data processor complies with security requirements.

7.2 Tasks and powers

No qualifications or experience are explicitly required to be appointed as a security officer. However, in view of his tasks, it must be ensured that he has experience in data protection security matters and that he is familiar with the corresponding organisation and IT systems. The security officer may be an employee or a third party.

The security document must appoint one or more security officers charged with coordinating and monitoring legal security measures. The appointment may be general for all databases and processing or it may be specific depending on the information systems used.

A security officer's main duty is to monitor compliance with the security measures when specific data are processed. Among others, he will analyse the audit reports and provide the data controller with his conclusions in order to allow the data controller to adopt the appropriate corrective measures. A security officer who controls access to sensitive data must review

access records on a monthly basis and draft a report on these reviews and the problems detected.

The appointment of a security officer does not waive the liability of the data controller or data processor and does not eliminate the need to satisfy registration requirements or to obtain the DPA's approval for data transfers and the processing of sensitive data.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Data transfers from Spain to recipients located in the European Economic Area (EEA) are not subject to additional requirements (they only need to be based on one of the legitimate grounds mentioned in section 3 above).

However, as a general rule, data transfers from Spain to recipients located outside the EEA require the prior authorisation of the DPA, unless the recipient officially ensures an 'adequate' level of protection as recognised by the European Commission (or the DPA) or the transfer can be based on a statutory exemption (see section 8.2 below).

Irrespective of the authorisation requirement, all international data transfers outside the EEA must be notified to the DPA for registration with the DPA's Registry.

8.2 Legal basis for international data transfers

Personal data may be transferred outside the EEA or outside an 'adequate' country/territory/system if:

- the transfer is the result of applying treaties or agreements to which Spain is a party; or
- the transfer serves the purposes of offering or requesting international judicial aid; or
- the transfer of data is related to money transfers in accordance with the relevant legislation; or
- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of precontractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject between the data controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds; or
- the transfer is necessary for the establishment, exercise or defence of a right in legal proceedings; or
- the transfer is necessary for medical prevention or diagnosis, the provision of health aid or medical treatment, or the management of health services; or
- the transfer takes place at the request of a person with a legitimate

interest, from a public register, and the request complies with the purpose of the register.

In all these cases, there is no need to obtain the DPA's prior authorisation.

8.2.1 Data transfer agreements

The authorisation of the DPA will be granted if the data exporter provides adequate safeguards, such as by concluding the European Commission's standard contractual clauses for data transfers. In Spain, data transfer agreements must be previously authorised by the DPA, even if they are based on these clauses.

8.2.2 Binding corporate rules

Spanish legislation expressly permits the DPA to grant authorisation based on binding corporate rules adopted within a group.

Spain is an MRP (Mutual Recognition Procedure) country and, thus, the BCRs approved by the leading data protection authority of any MRP country must be recognised in Spain.

However, this recognition is not automatic. The authorisation is only granted if the data exporters that are subject to Spanish regulations provide 'sufficient guarantees' to the DPA. As is the case with the EU Model Clauses, the BCRs are deemed 'sufficient guarantees' provided that they: (i) comply with 'the principles and the exercise of the rights set out' in the Spanish data protection regulations; and (ii) 'are binding and enforceable within the group according to the Spanish legal system'.

The subject matter of the DPA authorisation is not the BCRs themselves but the right of specific Spanish exporters to export specific data (contained in registered specific databases) to specific importers (of the same group as the Spanish exporters) and for specific purposes, according to specific guarantees (ie, the BCRs).

The granting of the authorisation entails per se that the BCRs become legal obligations and, as such, may be enforced by the data subjects and the Spanish DPA. In any event, 'authorised BCRs' do not replace any obligation under Spanish data protection.

8.2.3 Safe Harbour

The DPA's authorisation is not required for the transfers to US recipients who adhere to the 'Safe Harbour Privacy Principles and FAQs'.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The data controller and any persons involved in the processing of personal data are subject to professional secrecy regarding such data for an indefinite period.

9.2 Security requirements

The data controller and the data processor (as specified in the processing agreement – see section 3.5 above) must implement appropriate technical

and organisational measures to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access, taking into consideration the state of the art, the nature of the data stored and the risks to which they are exposed by virtue of human action or their physical or natural environment. The data controller must clearly define the functions and obligations of the persons having access to personal data, which they must indisputably acknowledge (as well as the consequence of their breach).

Specific security measures are imposed as a minimum for automated and non-automated databases under Royal Decree 1720/2007, which distinguishes between three levels of security measures (basic, medium and high) which are cumulative (that is, each database at a higher level must meet the requirements of that level as well as those imposed at all lower levels):

- Basic security level: all databases containing personal data.
- Medium security level: databases containing data on infringements of administrative or criminal regulations, Treasury data, and those related to the rendering of financial services on equity and credit solvency; as well as a series of personal data sufficient to enable an evaluation of the personality of the data subject (in this latter case, only the 'medium level' measures related to audit, identification and authentication, control of physical access and management of media apply).
- High security level: databases containing data on racial origin, political, religious or philosophical beliefs, data concerning health or sex life; as well as data collected for police purposes without the consent of the data subjects.

Databases whose controllers provide electronic communications services or operate public electronic communications networks must implement, in addition to the medium and basic security measures, an access record (which is a high level security measure) regarding traffic and location data.

<table>
<tr><th>Level</th><th>Automated</th><th>Non-automated</th></tr>
<tr><td rowspan="2">Basic</td><td colspan="2">• Security document: describes the mandatory technical and organisational security measures for employees who access the databases.
Inform the employees who access the data of the measures and the consequences of breaching them.
• Record of incidents.
• Rules for the management of devices containing the data and documents which allow the identification of the personal data contained in them and avoid theft, loss or unauthorised access during their transportation.
• Access control: updated list of authorised users and access histories.</td></tr>
<tr><td>• Identification and authentication measures (eg, passwords).
• Back-up procedures.</td><td>• Filing criteria.
• Mechanisms to prevent the access to storage devices or documents with personal data that are not contained in them.</td></tr>
</table>

Medium	• Appointment of one or more security officers to coordinate and monitor the security measures. • Audit.	
	• Registration of the entry and departure of devices containing personal data. • Limiting unauthorised access attempts. • Physical control over access. • Record of incidents, itemising the recovery processes carried out.	Not applicable
High	• Specific labelling rules of devices containing personal data to be encoded for transportation. • Backup copies and recovery procedures stored in a different location. • Access record, itemising every access attempt. • Encryption (when transmitted through telecommunication networks).	• Storage of information in areas to which access is protected (eg, locks, etc). • Possession of copies restricted to authorised personnel and destruction of those to be discarded. • Access to documents limited to authenticated personnel. • Measures to prevent access or manipulation of the information when transferring documents

9.3 Data security breach notification obligation

In addition to the incidents registry described in section 9.2, Article 34 of the Telecommunications Act establishes that 'in the event of a specific risk of a violation of the security electronic communication public network, the provider of a public communications network or a publicly available electronic communications service must inform subscribers of the existence of that risk and the measures to be adopted.'

This provision will be amended once the notification provisions on breach under Directive 2009/136/EC are transposed into Spanish law. On 27 May 2011, the Spanish government published a draft legislation amending this provision of the Telecommunications Act.

9.3.1 Who

According to the current wording of Article 34 of the General Telecommunication Law: a public communications network provider or that of a publicly available electronic communications service.

9.3.2 What

Risk of violating the security electronic communication public network and the measures to be adopted.

9.3.3 To whom

The subscribers.

9.3.4 When
At the time the provider becomes aware of the risk.

9.3.5 How
Not specified.

9.3.6 Sanctions for non-compliance
Under the current wording of the Telecommunications Act, failure to notify the security breach by the provider of a public communications network or a publicly available electronic communications service is deemed to be:

- a very serious infringement (if the failure is serious and repeated) and may be sanctioned with: (i) fines ranging from one to five times the gross benefit obtained as a result of the infringement or, if this criteria cannot be applied, a maximum fine of EUR 2,000,000; and (ii) professional disqualification of up to five years; or
- a serious infringement (if not considered a 'very serious infringement') and may be sanctioned with: (i) fines ranging from one to two times the gross benefit obtained as a result of the infringement or, if this criteria cannot be applied, by a maximum fine of EUR 500,000; and (ii) public warnings published in the Spanish Official Gazette and two newspapers with national circulation.

9.4 Data protection impact assessments and audits
9.4.1 Who
The data controller and the data processor must carry out audits, when required.

9.4.2 What
There is a legal requirement to conduct audits on security measures when the processing relates to data contained in databases that must conform to medium and high security measures (see section 9.2 above).

Furthermore, the security document must be kept updated and periodic monitoring obligations exist on back up/data recovery procedures and the access registry.

9.4.3 When
Audits must be carried out every two years. On an exceptional basis, the audit must be carried out when there are substantial modifications to the information system that could affect compliance with the implemented security measures.

9.4.4 How
Audits can be carried out either internally or externally. The audit report will be analysed by the security officer, who will communicate the conclusions to the data controller and will remain at the disposal of the DPA.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The DPA is the authority responsible for supervising the application of the DP Act and therefore has jurisdiction to inspect any processing, even if the database has not been registered.

10.2 Sanctions

The DPA supervises the application and enforcement of the DP Act and related regulations, whether *ex officio* or as a result of complaints.

Infringements and sanctions of the DP Act are classified as minor, serious and very serious and the corresponding fines are as follows:

- Minor infringements (eg, failure to register a database): from EUR 900 to 40,000 (and possibility of reprimand), with a prescription period of one year.
- Serious infringements (eg, processing of non-sensitive data not based on a legitimate ground or defective security measures): from EUR 40,001 to 300,000 (and possibility of reprimand), with a prescription period of two years.
- Very serious infringements (eg, processing of sensitive data not based on a legitimate ground or illegal transfers outside the EEA): EUR 300,001 to 600,000, with a prescription period of three years.

The Spanish Criminal Code establishes significant pecuniary fines (as a general rule, up to 24 months) as well as the possibility of imprisonment (as a general rule, up to four years) for the following criminal infringements relating to data protection:

- To seize – with the intention to discover secrets or to breach the privacy of another person – his papers, letters, email or any other documents or personal belongings, to intercept his telecommunications or to use technical devices for listening, transmitting, recording or reproducing sounds or images, or any other communication signal, without his consent.
- Unauthorised: (i) seizure, use or amendment, to the detriment of a third party, of personal or familiar reserved data that are recorded on computer, electronic or telematic files or media, or on any other kind of file, whether public or private; or (ii) access to data by any means or alteration or use to the detriment of the data subject or a third party.
- Unauthorised access to computer data or software within a computer system, or part thereof, in breach of the security measures established to prevent such access.
- Disclosure of secrets discovered as a result of professional activity or labour relationship.
- In order to discover a company secret, to obtain data, written or electronic documents, computer media or other objects related thereto, or use of telecommunications or technical devices for listening, transmitting, recording or reproducing sounds or images or any other communication signal.

The maximum daily fine is EUR 400 for individuals and EUR 5,000 for

legal entities.

Other laws, such as the Telecommunications Act and the E-Commerce Act establish other provisions regarding infringements and sanctions on data protection.

10.3 Examples of recent enforcement of data protection rules

The fines imposed by the DPA in 2010 amounted to EUR 17.5 million approximately in total. EUR 15 million were imposed on companies in the telecommunications and financial sectors and utilities as well as to spam and video surveillance activities.

10.4 Judicial remedies

Interested parties may appeal the DPA resolutions in administrative courts.

The DP Act provides data subjects with standing to claim damages arising from the violations of their data protection rights in civil courts. Claims for civil damages usually involve moral damages linked to the violation of honour (such as the improper inclusion of a debt in a credit history) and privacy rights (such as the dissemination of private images). In general, indemnities granted to date have not exceeded EUR 3,000.

The DPL does not provide for judicial remedies that must be enforced before the courts. The data subjects may address a claim to the DPA, but even if the DPA decides to start an investigation or a penalty procedure, the data subject shall not be 'a party' to it. As mentioned in section 5.1.2, they may also ask the DPA to order the controller to answer a request regarding access, rectification, cancellation and objection if he failed to do it beforehand or provided a defective answer.

10.5 Class actions

No specific class actions have been recognised for data protection matters. However, consumer protection regulations regulate class actions that have been used by consumer organisations to request that specific data protection clauses be overturned on the basis that they consider them to be unfair.

10.6 Liability

Data controllers are liable for damages resulting from any breach of the DP Act. However, if data processors breach the processing agreement, they will be deemed to be data controllers and will therefore be deemed personally liable.

Sweden

Mannheimer Swartling Erica Wiking Häger
Mikael Moreira & Anna Nidén

1. LEGISLATION

1.1 Name/title of the law

The collection and use of personal data is governed by the Personal Data Act (*Personuppgiftslag (1998:204))* (the PDA). The PDA implements the Directive 95/46/EC (the Directive). The PDA is supplemented by a Personal Data Ordinance, the Swedish Data Inspection Board's (*Datainspektionen*) (the Board) own statute book (*Datainspektionens föreskrifter*) (the Statute Book), and various pieces of legislation, including, but not limited to:

- The Debt Recovery Act *(Inkassolagen (1974:182));*
- The Credit Information Act *(Kreditupplysningslagen (1973:1173))*;
- The Electronic Communications Act *(Lagen (2003:389) om elektronisk kommunikation)* (the ECA); and
- The Patients' Personal Data Act *(Patientdatalag (2008:355))*.

1.2 Pending legislation

There is no pending legislation further to the PDA. There are however several proposed amendments to various pieces of legislation. The more important ones are:

- A new Camera Surveillance Act *(Lagen (1998:150) om allmän kameraövervakning)* (the CSA) is proposed that grants the Board supervisory powers in relation to the CSA. It is also proposed that the Board assumes the Chancellor of Justice's *(Justitiekanslern)* right to appeal camera surveillance decisions.
- It is proposed that Directive 2006/24/EC (the Data Retention Directive) is implemented into Swedish legislation. Under the proposal it would be mandatory to store certain information that is generated or processed as a result of phone calls, text messaging and internet traffic. The proposal was expected to enter into force on 1 July 2011 but the decision to implement the proposal has been postponed for one year.
- A new Police Data Act *(Polisdatalag (2010:361))* is proposed and expected to enter into force on 1 March 2012. The new Act will replace the current Police Data Act *(Polisdatalag (1998:622))*. The new Act will address various difficulties that the current Act has been shown to give rise to, for example, in relation to the possibility to process personal data in order to prevent and detect criminal activity. The new legislation also creates conditions for better cooperation between national law enforcement authorities by allowing increased information exchange.

1.3 Scope of the law

1.3.1 The main players

- The 'data controller' is a person who alone, or together with others, decides the purpose and means of processing personal data. The data controller is usually a legal entity, but can also be an individual.
- The 'data processor' is any natural or legal person, private or public body, which processes personal data on behalf of the data controller.
- The 'data subject' is the natural person whose personal data are being processed.
- The 'data protection officer' is appointed by the data controller and is responsible for independently ensuring that the data controller processes personal data in a lawful and correct manner and in accordance with good practice.
- A 'third party' is a person other than the data subject, the data controller, the data processor, the data protection officer and such persons who under the direct responsibility of the data controller or the data processor is authorised to process personal data.

1.3.2 Types of data

'Personal data' are any information that directly or indirectly may reference a natural person who is alive. Anonymised personal data that can be related to a particular data subject when combined with other relevant bits of data are therefore considered personal data. For example, an internet protocol address (IP address) is deemed personal data as long as the IP address in conjunction with additional information (such as an internet provider's billing information) can identify the individual using the IP address. Encrypted personal data are also considered personal data and subject to the PDA for as long as someone has the ability to decrypt the personal data.

The PDA does not cover information relating to non-living individuals such as deceased persons or people not yet born. The same applies for information relating to legal persons (corporate entities) even if the legal person has a company name, or a limited number of owners, that would make it possible to identify a natural person. However, information regarding a sole trader *(enskild firma)* is considered personal data as a sole trader always has a sole natural person as the owner.

In addition the PDA refers to other types of personal data that are subject to special rules:

- Sensitive personal data. Sensitive personal data are defined by the PDA to include information on: (i) race or ethnic origin; (ii) health and sex life; (iii) political opinions; (iv) religious or philosophical beliefs; and (v) trade union membership.
- Personal identity numbers. In Sweden, each natural person is assigned a personal identity number at birth.
- Judicial data. This would, for example, include information regarding crimes and verdicts in criminal cases.

1.3.3 Types of acts/operations

The PDA applies to automatic processing of personal data and, in certain

cases, manual processing of personal data on traditional paper-based files such as manual registers or filing systems. The PDA applies both to the public and private sector and contains provisions to protect individuals' privacy from being violated by the processing of personal data. The following are examples of operations that constitute processing of personal data: collection; recording; organisation; registration; storage; processing; disclosure by transfer or dissemination of personal information; and compilations or joint processing of personal data.

Personal data can only be processed for specific, explicitly stated and legitimate purposes. Personal data cannot be reprocessed for any purpose that is incompatible with the original purpose, meaning that data that have been gathered for a particular purpose cannot be processed later for a different purpose or in a different manner.

The application of the PDA does not require that the information processed is structured in a specific way or is being processed by any particular method, therefore all computerised work and text processing, or similar processing of running text containing personal data would be subject to the PDA. However, in order to facilitate the processing of personal data that generally would not entail any violation of personal privacy, simplified rules apply to unstructured material. Unstructured material can, for example, consist of running texts, sound, images, email messages, texts published on the internet or text produced with word processing software as long as the data are not included, or intended to be included, in any system capable of structuring the data, such as a database. The simplified rules mean that the majority of the PDA's provisions do not apply when processing personal data in unstructured material. For example, the data controller is not required to comply with: (i) the fundamental requirements of the PDA; (ii) the restrictions regarding transfer of data to countries outside the EU and the EEA; or (iii) the information requirements, including data subject access rights.

The simplified rules constitute 'abuse rules', meaning that the above exemptions when processing personal data in unstructured material only apply if the privacy of the data subject is not violated. This means that a data controller which processes personal data on the basis of the abuse rules must not: (i) process personal data for improper purposes, such as persecution; (ii) compile a large quantity of data about one person without acceptable reasons; (iii) fail to correct personal data which prove to be incorrect or misleading; (iv) defame or insult another person; or (v) breach a duty of confidentiality.

If the Board deems that the data controller misuses the processing of personal data in unstructured material, the PDA will apply in its entirety.

1.3.4 Exceptions

The PDA does not apply to personal data that an individual collects and maintains in an activity of a purely private nature. For example, an individual is permitted to maintain an electronic diary or a register with the addresses of friends and relatives.

In addition there are exceptions related to official documents from public authorities, the freedom of the press and the freedom of expression and also for certain processing of personal data related to journalistic work, or artistic or literary creations (see section 1.4 below).

1.3.5 Geographical scope of application

The PDA applies to data controllers established in Sweden. In addition, the PDA applies to data controllers who are established in a country outside the EU and the European Economic Area (EEA), but use equipment situated in Sweden to process personal data. In such cases the data controller must appoint a representative established in Sweden. The provisions in the PDA concerning data controllers also apply to the representative.

The PDA does not apply if equipment is used only to transfer information between two countries that are both located outside the EU/EEA.

1.4 Particularities

Under Swedish law, there is a constitutional principle of access to official documents. This means that public authorities have a duty to disclose public documents upon request (unless secrecy applies), and also to archive and save public documents without alterations. The provisions of the PDA cannot be applied to limit the principle of access to official documents. In addition, the provisions concerning freedom of the press and freedom of expression in the Freedom of the Press Act *(Tryckfrihetsförordningen (1949:105))* and the Fundamental Law on Freedom of Expression *(Yttrandefrihetsgrundlagen (1991:1469))* also prevail over the provisions of the PDA.

As stated in section 1.3.3, in order to facilitate the processing of personal data that generally would not entail any violation of personal privacy, simplified rules apply to unstructured material.

2. DATA PROTECTION AUTHORITY

Datainspektionen (Data Inspection Board)
P.O. Box 8114
104 20 Stockholm
Sweden
T: +46 (0) 8 657 61 00
F: +46 (0) 8 652 86 52
E: datainspektionen@datainspektionen.se
W: *www.datainspektionen.se*

2.1 Role and tasks

The Board is a governmental authority. Its task is to protect the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. The Board supervises the compliance of authorities, companies, organisations and individuals with the PDA and certain other legislation such as the Debt Recovery Act and the Credit Information Act.

The Board assists individuals whose privacy has been infringed, and

issues directives, codes of statues and general recommendations, as well as opinions on legislative proposals. The Board also handles complaints and carries out inspections. By examining government bills the Board ensures that new laws and ordinances protect personal data in an adequate manner.

2.2 Powers

The Board has the following powers. It may upon request obtain:

- access to personal data processed by a data controller;
- information about and documentation of the processing of personal data;
- information on the security of the processing of personal data; and
- access to the premises connected with the processing of personal data.

If the Board concludes that the processing of personal data is unlawful, or is unable to obtain sufficient guarantees that the processing of personal data is lawful, the Board can prohibit a data controller from processing personal data in any manner other than by storing it (subject to a default fine).

In addition the Board has the power to grant default fines if a data controller does not voluntarily comply with decisions by the Board concerning security measures that have entered into final force and effect. The Board may also apply to the County Administrative Court for the erasure of such personal data that have been processed in an unlawful manner.

2.3 Priorities

The Board adopts a new management plan each year. The management plan includes a list of priority areas on which the Board will focus in the upcoming year. The Board tries to focus on sensitive areas, new phenomena and areas where the risk of misuse of data is particularly great. In 2010 a lot of the Board's focus and recourses were put into controlling how, from a privacy perspective, the National Defence Radio Establishment (FRA) processes personal data in connection with signals intelligence in defence intelligence.

For the year 2011 the Board has stated that it will pay particular attention to the following areas: online abuse; online credit reporting services; and new surveillance and identification technologies.

In 2011 the Board has, together with other data protection authorities in the Nordic region, sent a request to Facebook (the world's largest social network) for the purpose of gaining information on how Facebook processes personal data. In addition, the Board has issued guidelines to clarify the requirements under the PDA in relation to cloud computing.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

The main rule under the PDA is that personal data and sensitive personal data can only be processed if the data subject has given his consent to the processing.

Consent from the data subject is valid provided that it is a voluntary,

specific and unambiguous expression of will, implying that the data subject, after the receipt of information, accepts the processing of personal data concerning him. The data subject must receive all information necessary to enable him to assess how the collected personal data will be used and the advantages and disadvantages of the processing, in order to be able to exercise his rights under the PDA. The consent must be specific, meaning that a data subject's consent only applies to a particular processing performed by a particular data controller for a particular purpose. Therefore it is not possible to obtain general consent.

3.1.2 Form

The PDA does not require consent to be given in a specific form; it can either be verbal or written. The burden of proof is on the data controller to show that consent has been given to the particular processing. It is therefore recommended that written confirmation be obtained by the data controller.

3.1.3 In an employment relationship

Consent in an employment relationship does not have to be given in a specific form, however, as an employee may often be in a position of dependence towards his employer, it is questionable whether the subordinate position of the employee prevents consent from being truly voluntary. Accordingly, the processing of personal data on the basis of consent should, in situations where an employer processes an employee's data, be limited to such situations where the employee has actual free choice and where the employee may withdraw his consent without adversely affecting his position.

3.2 Other legal grounds for data processing

There are other legal grounds for the processing of personal data and sensitive personal data besides obtaining consent from the data subject.

Processing of personal data is permitted, without the data subject's consent, if the processing is necessary to:

- enable the performance of a contract with the data subject, or to enable measures that the data subject has requested to be taken before a contract is entered into;
- enable the data controller to comply with a legal obligation;
- protect the data subject's vital interests;
- act in the public interest;
- enable the data controller, or a third party to whom the personal data are provided, to act in conjunction with the exercise of official authority; or
- satisfy a purpose that concerns a legitimate interest of the data controller, or of a party to whom personal data are provided, if this interest is of greater weight than the privacy interest of the data subject.

Processing of sensitive personal data is permitted if:

- the data subject has given his explicit consent to the processing, or has made available and published the personal data in a clear manner;

- the processing is necessary to ensure that the data controller is able to: (i) fulfil obligations or exercise rights under employment law; (ii) protect the data subject's vital interests, and the data subject cannot provide his consent; or (iii) establish, exercise or defend legal claims;
- the processing is within the operation of non-profit organisations with political, philosophical, religious or trade union objectives. (However, the sensitive personal data cannot be disclosed to a third party without the data subject's consent); or
- the processing is necessary for preventive medicine, medical diagnosis, healthcare or treatment, or the administration of health and hospital care.

It is also generally prohibited for any person or party other than public authorities to process personal data concerning judicial data such as violations of laws involving crimes and judgments in criminal cases, coercive penal procedure and so on. The government or the Board can issue exemptions from the prohibition on processing sensitive personal data and personal data concerning judicial data where such exemptions are necessary for the public interest.

Data concerning personal identity numbers can be processed without consent only when manifestly justified, with regard to the purpose of the processing, the importance of secure identification or some other substantial reason.

3.3 Direct marketing and cookies

The processing of personal data for the purpose of direct marketing is subject to the general provisions of the PDA. The PDA explicitly states that the data subject can at any time object to the processing of personal data for the purpose of direct marketing by notifying the data controller. After the data subject's notification, no subsequent processing of the data subject's personal data for the purpose of direct marketing can be conducted by the data controller.

In addition, the Marketing Practices Act *(Marknadsföringslagen (2008:486))* (the MPA) also contains certain provisions regarding the use of personal data for direct marketing purposes. A trader can use email, facsimile, or other similar automated systems for direct communication with a data subject for marketing purposes only if the data subject has consented to it beforehand. However, consent is not necessary if the personal data have been collected in connection with a sale of a product to a customer provided that the customer has not objected to the data being used for marketing purposes at the time the data were collected and the marketing message refers to the traders own, similar products.

The ECA applies to service providers of electronic communications networks and communications services. The ECA stipulates that provided that cookies are not required or necessary in order to provide a service, all visitors to a website must consent to a cookie being used. The information provided to visitors about the use of cookies should as a minimum contain information about the type of cookie used, which domain the cookie belongs to, which data are stored in the cookie and how long the cookie is saved in the visitor's web browser. It should be mentioned that as the current rules have been changed recently (as of 1 July 2011) in order to

implement the changes brought about to the ePrivacy Directive by Directive 2009/136/EC of 25 November 2009, it is still unclear how the new rules on cookies will be interpreted by authorities and how they will be applied in practice.

3.4 Data quality requirements

The data controller must ensure that personal data are, at all times:

- processed only if it is lawful;
- processed in a correct manner and in accordance with good practice;
- only collected for specific, explicitly stated and justified purposes;
- not processed for any purpose that is incompatible with the purpose for which the information was gathered;
- adequate and relevant for the purposes of the processing;
- not excessive – only the required sets of personal data can be processed and they must be linked to the purposes of the processing;
- correct and up to date;
- rectified, corrected, blocked or erased, if they are incorrect or incomplete with regard to the purpose of the processing; and
- not kept for a longer period than necessary with regard to the purpose of the processing.

3.5 Outsourcing

When outsourcing data processing activities to data processors, the data controller is required to enter into a written agreement with the data processor. The agreement must contain provisions stipulating that: (i) the data processor may only process the personal data on the instructions of the data controller; and (ii) the data processor shall comply with the security measures stipulated in the PDA.

If the data processor intends to sub-contract the data processing to a sub-data processor, the data controller must ensure that the same obligations that apply to the data processor apply to the sub-data processor. This means that the data controller must have written agreements in place with both the data processor and the sub-data processor.

If the outsourcing includes the use of cloud computing services, the data controller should comply with the Board's specific guidelines for cloud computing services (issued in September 2011).

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use as well as the use of surveillance cameras is subject to the provisions of the PDA, the ECA and the CSA.

The ECA contains important restrictions on intercepting electronic communications during transfer, including listening in on telephone conversations, as well as monitoring email messages before they reach the recipient. The ECA also imposes specific obligations on accessing information stored on a user's computer (or other equipment), such as cookies, or using an electronic communications network.

The CSA stipulates that camera surveillance may only be conducted if the data subjects' privacy is respected. Permission is required, with some exemptions, from the County Administrative Board *(Länsstyrelsen)* to use cameras that monitor public places. In some premises like banks and shops only a registration by the County Administrative Board is needed provided that the purpose of the camera surveillance is to prevent crimes and the installed cameras are fixed and placed by the register and/or by the entries and exits. Permission to use camera surveillance is granted by the County Administrative Board provided that the interests of the surveillance outweighs the individual's interest not to be monitored.

3.6.2 Employment relationship

The PDA allows the monitoring of employees' usage of internet and email provided that:

- the employee has given his or her consent;
- there is an agreement between the employer and the employee; or
- it is necessary in order to fulfil a legal duty; or
- the data controller has a legitimate interest to monitor and that such interest is of greater weight than the interest of the employees in protecting against violations of their personal privacy.

The employer must inform the employees about what kind of processing of personal data can and will take place in connection with internet and email surveillance. The obligation includes having guidelines regarding such surveillance, however there is no obligation to inform the employee on every occasion surveillance control takes place.

There have to be very strong reasons for handling personal data if the employee has explicitly objected to it. In addition, if the employer notices that the monitored email is of a strictly private nature the employer has to stop reading it immediately.

A data controller does not need any permission in order to install surveillance cameras in areas without public access. However, it is possible that such instalment is not in accordance with the PDA as camera surveillance always involves an intrusion into the privacy of the monitored individuals. In order for the monitoring to be permitted it has to be determined whether the intrusion is permissible. The data controller must weigh up whether the intrusion of privacy is a proportionate measure in relation to the interests that prompt the instalment of the surveillance. It is necessary to inform the employees about the purpose of the surveillance and how long the data are being stored. The information can be given to the employees in connection with their hiring and/or when the cameras are being installed. The information should preferably also be available on, for example, the corporate intranet.

4. INFORMATION OBLIGATIONS

4.1 Who

It is the data controller that is responsible for informing data subjects about data processing.

4.2 What

The information to be provided by the data controller must include:

- the name, address, telephone number, company registration number and email (to the extent applicable) of the data controller;
- information concerning the purpose of the processing; and
- all other information necessary for the data subject to be able to exercise his rights in connection with the processing.

This means that the information provided by the data controller must include information about the recipients of the personal data, and that the data subject is entitled to request information from the data controller concerning the processing and that the data controller is obliged to rectify any erroneous information about the data subject. The information must be provided voluntarily by the data controller.

4.3 Exceptions

There are exceptions to a data subject's right to receive information. Information does not need to be provided in relation to matters about which the data subject is already aware. Where the personal data are collected from a third party and not from the data subject himself, it is not necessary to provide information to the data subject if it: (i) is impossible: and/or (ii) would involve a disproportionate effort.

When assessing whether the effort is disproportionate or not, the following factors are taken into account:

- the number of data subjects;
- the personal data's age; and
- any measures that may need to be taken in order to protect the data subject.

The obligation to provide information to the data subject can also be limited by legislation. For example, confidentiality of health and hospital care can apply to the data subject (for example a patient) with regard to the purpose of the care or treatment.

4.4 When

If personal data about a data subject are collected from the data subject himself, the data controller must provide the information to the data subject at the point of collecting the data subject's personal data.

If personal data have been collected from a source other than the data subject himself, the main rule is that the data controller must provide the data subject with information about the processing of the data when the data are registered by the data controller.

4.5 How

The information can be either verbal or written, however, the burden of proof is on the data controller to show that it has provided sufficient information. It is therefore recommended that written confirmation be obtained by the data controller that the data subject has received the information.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Upon request from a data subject, the data controller must provide information on whether personal data concerning the data subject are being processed or not. If personal data are processed, written information must also be provided about:

- which information is being processed;
- the source from which it was collected;
- why the processing is taking place; and
- to which recipients or groups of recipients the data are being disclosed.

The data subject's application to receive information must be made in writing to the data controller and be signed by the data subject himself. The right for the data subject to request information is limited to one occasion per calendar year.

5.1.2 Exceptions

Information does not need to be provided about personal data in running text that has not been given its final wording when the application was made or for text that acts as a memory aid or the like. However, this exception does not apply if: (i) the data have been disclosed to a third party; (ii) the data were only processed for historical, statistical or scientific purposes or; (iii) regarding running text that has not been given its final wording, if the personal data have been processed for a period longer than one year.

5.1.3 Deadline

The data subject can exercise the right to request information at any time. The data controller must submit the information to the data subject within one month of the request. However, if there are special reasons for doing so, the information may be provided not later than four months after the application was made. Special reasons may for example be that the personal data are encrypted or that the personal data are divided into different data files.

5.1.4 Charges

The information shall be provided free of charge to the data subject.

5.2 Rectification

5.2.1 Right

The data subject has the right to request that any personal data that have not been processed in accordance with the PDA are immediately rectified. The data controller must also notify any third party to whom personal data have been disclosed about the measures taken if requested to do so by the data subject, or if such notification would prevent substantial damage or inconvenience to the data subject.

In the case of disagreement over whether data should be corrected or not, the data subject can report the matter to the Board. In addition, the data subject can bring an action with the administrative court against the data

controller and sue for damages if the data controller does not rectify such personal data that have not been processed in accordance with the PDA.

5.2.2 Exceptions

No notification to third parties is needed if it proves impossible or would involve a disproportionate effort.

5.2.3 Deadline

The data controller must rectify the personal data immediately upon receiving the data subject's request. This means that the data controller for example cannot justify any postponements because the personal data will be rectified 'soon enough' through a scheduled update if it is possible to update the personal data earlier.

5.2.4 Charges

The personal data shall be rectified free of charge.

5.3 Erasure

5.3.1 Right

Any data subject has the right to request erasure of any personal data relating to him, under the same conditions as the right to request rectification.

5.3.2 Exceptions

The same exceptions apply as for rectification.

5.3.3 Deadline

The same deadline applies as for rectification.

5.3.4 Charges

The personal data shall be erased free of charge.

5.4 Blocking

5.4.1 Right

Any data subject has the right to request that the data controller blocks personal data relating to him, under the same conditions as the right to request rectification.

5.4.2 Exceptions

The same exceptions apply as for rectification.

5.4.3 Deadline

The same deadline applies as for rectification.

5.4.4 Charges

The personal data shall be blocked free of charge.

5.5 Objection

5.5.1 Right

The data subject can withdraw his consent to further data processing by notifying the data controller. In addition, the data subject can always object to the processing of personal data for direct marketing.

5.5.2 Exceptions

The data subject does not have a general right to object to processing of his personal data for such processing that is allowed under the PDA.

5.5.3 Deadline

The data controller must immediately stop the processing of personal data upon the data subject's objection. After the data subject's notification, no subsequent data processing of the data subject's personal data may be conducted by the data controller.

5.5.4 Charges

The data subject may not be charged for his right to object to further processing.

5.6 Automated individual decisions

5.6.1 Right

If a decision that has a legal effect on a data subject (or otherwise materially affects a data subject) is based solely on automated processing of such personal data that are intended to assess the data subject's qualities, the data subject must upon request have an opportunity to have the decision reconsidered by a natural person.

5.6.2 Exception

Not applicable.

5.6.3 Deadline

There are no specific rules in the PDA regarding how much time the data controller has to reconsider the decision. However, a commentary to the PDA suggests that it should be made without undue delay.

5.6.4 Charges

The data subject's right to have the decision reconsidered by a person shall be free of charge.

5.7 Other rights

5.7.1 Right

There are no other rights.

5.7.2 Exception

Not applicable.

5.7.3 Deadline
Not applicable.

5.7.4 Charges
Not applicable.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who
The data controller must provide a written notification to the Board before any processing, or a set of processing with a similar purpose, is conducted.

6.1.2 What
The general rule is that all processing of personal data that is completely or partially automated is subject to a notification duty under the PDA.

6.1.3 Exceptions
Notification is not required if the data controller has appointed a data protection officer (see section 7 below).

In addition, the government, or an authority appointed by the government, can grant exemptions from the duty of notification in certain cases, and for certain kinds of processing which are not likely to result in an improper intrusion of privacy. Under the Statute Book, various types of processing are exempt from the general notification duty, for example:

- processing of personal data in unstructured material (see section 1.3 above);
- processing that the data subject has given consent to;
- processing relating to data subjects who are associated with the data controller by reason of membership, employment, a customer relationship or similar relationship, provided the processing does not relate to sensitive data;
- processing by employers that relates to employees' sick leave periods, provided the data are used for salary administration purposes or to determine whether the employer must undertake a rehabilitation investigation;
- processing by employers that reveals employees' trade union memberships, provided the data are used to enable employers to fulfil obligations or exercise rights under labour law or to make it possible to determine, enforce or defend legal claims;
- processing of personal data collected from data subjects where processing is essential for compliance with the provisions of laws or regulations;
- processing of personal data which can be processed in the health care sector under provisions in the PDA; and
- processing of personal data used in the activities of lawyers that are relevant to the provision of their services and to avoid conflicts of interest.

Members of trade organisations can avoid the notification duty (and instead hold their own registers of the processing of personal data that the data controller conducts) provided that their trade agreements have been reviewed and approved by the Board. Examples of trade organisations which have had their trade agreements approved are the direct marketing association (SWEDMA), the Swedish Debt Collection Association *(Svensk Inkasso)* and the Swedish Property Federation *(Fastighetsägarna)*.

6.1.4 When
Notification must be made before any processing of personal data is made.

6.1.5 How
Notification is made to the Board by using an application form that is available on the Board's website.

6.1.6 Notification fees
Notification is free of charge.

6.2 Authorisation requirements
There are no authorisation requirements regarding processing of personal data under Swedish law. However, as stated in section 3.2 it is prohibited for parties other than public authorities to process personal data concerning legal offences involving crime and verdicts in criminal cases. The Board may in individual cases decide to grant an exemption from this prohibition.

A group of companies with binding corporate rules (see section 8.2.2 below) must have the binding corporate rules pre-approved by the Board by way of application. There are no formal requirements on how such application shall be made or filed. The Board does not abide by the mutual recognition procedure for the approval of binding corporate rules.

6.2.1 Who
Not applicable.

6.2.2 What
Not applicable.

6.2.3 Exceptions
Not applicable.

6.2.4 When
Not applicable.

6.2.5 How
Not applicable.

6.2.6 Authorisation fees
Not applicable.

6.3 Other registration requirements

The government may issue regulations that processing personal data which entails particular risks regarding the intrusion on a data subject's privacy must be notified in advance to the supervisory authority. For example, notification in advance is required: (i) when processing personal data including information on genetic predispositions; (ii) when the Swedish Tax Agency processes personal data in connection with criminal investigations; and (iii) for certain processing by the Swedish police, Swedish customs and the Swedish coast guard. Notification for the above mentioned cases must be made three weeks in advance of commencing the processing.

6.4 Register

The reported data will be registered with the Board and are available to the public. The register is a public document and the public can access the register by contacting the Board.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The data protection officer is responsible for independently ensuring that the data controller processes personal data in a lawful and correct manner and in accordance with good practice. Under the PDA it is not mandatory to appoint a data protection officer. However, if a data controller appoints a data protection officer, the notification requirements to the Board are no longer mandatory.

A data protection officer is appointed by giving notice to the Board identifying the data protection officer. A data controller must keep the Board informed of all changes by notifying it of any new appointment or removal of a data protection officer.

It is common in Sweden that organisations appoint data protection officers. Usually this is done in order to avoid the notification requirements described in section 6.1.

7.2 Tasks and powers

The data protection officer must independently ensure that the data controller processes personal data in a lawful and correct manner and in accordance with good practice. The data protection officer must also point out any inadequacies to the data controller. If the data protection officer has reason to suspect that the data controller is in breach of data protection legislation and no rectification is made to the breach by the data controller after being notified by the data protection officer, the data protection officer must notify such breach to the Board. The PDA does not require a notification to be given in a specific form.

The data protection officer must maintain a register of the processing that the data controller conducts, and which would have been subject to notification to the Board if the data protection officer had not been appointed. The register must as a minimum contain the information that a

notification made by a data controller to the Board would have contained.

The data protection officer may also consult with the Board if in doubt about how applicable data protection legislation is to be applied.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Generally, it is prohibited to transfer personal data that are being processed to a country outside the EU/EEA which does not have an adequate level of protection for personal data. When assessing the level of protection afforded by a country outside of the EU/EEA, all circumstances surrounding the transfer are considered. However, particular consideration must be given to the:

- nature of the data;
- purpose of the processing;
- duration of the processing;
- country of origin;
- country of final destination; and
- rules that exist for processing in the third country.

Whether the level of protection in a particular country is adequate must be assessed on a case-by-case basis. It is possible for a country to have an adequate level of protection in certain fields, but not in others.

8.2 Legal basis for international data transfers

It is permitted to transfer personal data to a country outside the EU/EEA if the data subject has given his consent to the transfer. Transfer to a country outside the EU/EEA is also permitted if the transfer is necessary for:

- performance of a contract between the data controller and the data subject, or measures that the data subject has requested to be taken before a contract is made;
- conclusion or performance of a contract between the data controller and a third party, which is in the data subject's interest;
- establishment, exercise or defence of legal claims; or
- protection of vital interests of the data subject.

It is also permitted to transfer personal data for use in a state that is a party to the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), provided that the personal data are used only in that particular state.

For automated processing, the government can issue regulations permitting transfer of personal data to a country outside the EU/EEA provided that the transfer is regulated by an agreement with sufficient guarantees for the rights of the data subject. The government considers that standard contractual clauses and binding corporate rules provide such sufficient guarantees (see 8.2.1 regarding data transfer agreements and 8.2.2 regarding binding corporate rules). In addition, the government can issue regulations, or decide on individual cases, to permit the transfer of personal data to a country outside the EU/EEA provided: (i) it is considered necessary, with regard to vital public interests; and

(ii) there are sufficient safeguards to protect the data subject's rights.

8.2.1 Data transfer agreements

The government can, in relation to matters of automated processing of personal data, issue regulations permitting the transfer of personal data to a party outside the EU/EEA, provided the transfer is regulated by an agreement that provides sufficient guarantees of the rights of the data subjects.

Sweden has acknowledged the validity of the three sets of standard contractual clauses approved by the European Commission. The Personal Data Ordinance expressly provides that a transfer of personal data to a country outside the EU/EEA is allowed when the transfer is subject to any of the three sets of standard contractual clauses. However, the transfer must always be in accordance with the general rules concerning the processing of personal data and the specific rules regarding sensitive personal data.

8.2.2 Binding corporate rules

A group of companies that has formally adopted binding corporate rules (BCRs) can also freely transfer personal data among their group of companies. The BCRs must be pre-approved by the Board (see section 6.2 above).

8.2.3 Safe Harbour

There is no need for an authorisation where the personal data are transferred to an organisation that is certified under the US Safe Harbour scheme and the data transfer falls into the scope of that certification.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

A data controller shall implement appropriate technical and organisational measures to protect the data processing and ensure the confidentiality and security of the personal data.

9.2 Security requirements

The security requirements in the PDA require measures that are appropriate with regard to:

- the technical possibilities available;
- the costs of implementing the measures;
- the specific risks associated with the processing of personal data; and
- how sensitive the processed data are.

When the data controller engages a data processor, the data controller has to make sure that the data processor will be able implement the security measures that have to be implemented as well as make sure that the data processor actually implements the measures.

The Board has issued non-binding guidelines concerning the security that is required by the PDA. The guidelines are recommendations on how the mandatory security requirements of the PDA can be satisfied. However, the Board can decide on measures a data controller must implement to satisfy

the PDA's security requirements. If the data controller fails to comply with such security measures, the Board can prescribe a default fine. The Board strictly enforces security matters and can, to a reasonable extent, provide advice on security matters to a data controller. The assessment of which security measures are needed to satisfy the PDA's requirements depend, among other things, on the type of personal data that are being processed.

9.3 Data security breach notification obligation

There is no obligation under the PDA requiring data controllers to notify breaches to the Board or to data subjects. However, if a data protection officer has been appointed he must under certain circumstances notify breaches of the PDA to the Board (see section 7 above).

Between the years 2008 and 2010 the Board received 844 complaints concerning breaches of the PDA, including complaints from both the public and data protection officers. The majority of complaints are received from the public.

In addition, a provider (normally the data controller) of publicly available electronic communication services such as a telecom carrier or an internet service provider shall, without undue delay, inform the Swedish Post and Telecom Agency *(Kommunikationsenheten PTS)* of any incidents involving privacy breaches. If the incident is likely to have a negative effect on the users affected by the privacy breach, or if the Swedish Post and Telecom Agency so requests, the provider must inform the data subjects without undue delay.

9.3.1 Who

Not applicable.

9.3.2 What

Not applicable.

9.3.3 To whom

Not applicable.

9.3.4 When

Not applicable.

9.3.5 How

Not applicable.

9.3.6 Sanctions for non-compliance

There are no specific sanctions under Swedish law for non-compliance.

9.4 Data protection impact assessments and audits

Information security is an important part of any data protection regime. Under the PDA the data controller must ensure that personal data within the organisation are protected by technical and organisational measures.

The Board recommends that a data protection security assessment should be made to assess the level of security appropriate within the organisation. A data protection impact assessment should be conducted as part of the general information security procedures and when particularly sensitive processing is planned. The Board states in its guidelines for cloud computing that such assessment must be made prior to using cloud services. The data controller may rely on generally established methods for data protection impact assessments, for example ENISA's Cloud Computing Information Assurance Framework.

The Board also recommends that the data controller ascertain a right to audit its data processors' compliance with applicable security requirements. Data processing agreements should include appropriate provisions on audit rights.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The main objective of the Board is to assist and advise data controllers to resolve any unlawful processing of personal data. If the Board finds that a data controller acts in breach of the PDA it can take action or issue a temporary decision subject to a default fine.

The Board can obtain, on request:

- access to personal data processed by a data controller;
- information about and documentation of the processing of personal data;
- information on security of the processing of the personal data; and
- access to the premises connected with the processing of personal data.

If the Board concludes that the processing of personal data is unlawful, or is unable to obtain sufficient guarantees that the processing of personal data is lawful, the Board can prohibit a data controller from processing personal data in any manner other than by storing it. The Board can also, at the County Administrative Court, apply for the erasure of personal data that have been unlawfully processed. The Board can also decide on measures that a data controller must implement to satisfy the Board's security requirements.

10.2 Sanctions

A natural person can be subject to a fine or imprisonment of up to two years if he:

- intentionally or by gross negligence discloses untrue data in information or notifications under the PDA;
- in contravention of the provisions of the PDA, processes sensitive personal data or data concerning violations of laws;
- transfers personal data to a country outside the EU/EEA in violation of the PDA;
- fails to notify the Board concerning the processing;
- processes sensitive data or, if not a public authority, personal data concerning legal offences including crime, judgments in criminal cases, coercive penal procedural measures or administrative deprivation of

liberty in violation of the data subject's privacy; or
- with respect to unstructured personal data violates the data subject's privacy by transferring data outside the EU/EEA to a country which does not have an adequate level of protection of personal data.

Normally the courts impose penalties in the form of fines and damages. The level of the fine depends on the severity of the infringement and the level of income of the individual responsible for the infringement. The fines applied by Swedish courts in this respect rarely exceed EUR 5,000. A sentence is not imposed in petty cases. As a result, imprisonment sentences are rare and the few imprisonment sentences rendered by Swedish courts have involved additional offences, such as defamation.

Before the Board decides to award a fine, the data controller must be given the opportunity to express and defend himself. If the matter is urgent, the Board can issue a temporary decision (subject to a default fine) until the data controller has been given the opportunity to defend himself. Decisions given by the Board can be appealed to the Administrative Court of Appeal.

10.3 Examples of recent enforcement of data protection rules

The Board normally focuses on investigating certain sector and industry areas each year concerning the processing of personal data.

The Board has, for example, reviewed how companies handle personal data in relation to recruiting activities as well as if and how camera surveillance in schools is in accordance with the PDA. The Board has also reviewed credit reporting companies in connection with new rules being implemented forcing data subjects to receive a copy when a credit information report is issued by a credit reporting agency. The Board has recently focused on employers who use GPS devices to map their vehicles' movements. A recurring error is that the information that employers provide to employees does not meet the legal requirements and is often imprecise and unclear.

10.4 Judicial remedies

A person suffering any harm as a consequence of acts infringing the provisions of the PDA can initiate a civil action for damages. Only the data subject and not his family or estate can be compensated. A data controller can also be subject to criminal charges if he has not handled the personal data in accordance with the PDA.

However, in Sweden it is not very common to initiate judicial proceedings. Breaches are usually solved directly with the Board.

10.5 Class actions

Class actions are permitted under Swedish law but are uncommon. No class action in relation to a breach of data protection laws has, to our knowledge, been initiated in Sweden.

10.6 Liability

The data controller shall be held liable for any damage as a result of an

action in violation of the PDA. Data subjects that have incurred damage from an action in violation of the PDA may thus claim damages from the data controller. The damages can be adjusted if the data controller proves that the act which caused the damage cannot be ascribed to him. Neither the data controller's employees nor data protection officers or third parties can be subject to a damage claim for actions in violation of the provisions in the PDA; only the data controller himself is liable for such claims.

In an example of recent case law, the Supreme Administrative Court (Case RÅ 2010 ref. 35) has approved camera surveillance outside the entrance of an apartment building. The Supreme Administrative Court found that in this particular case it was the visitors' choice to call on the buildings' door phone (thereby activating the surveillance camera) and that the images that the camera conveyed were limited in area. As only the apartment called could see the images and for a short period of time the privacy intrusion was considered to be limited by the Supreme Administrative Court. The interests of the tenant association were considered to outweigh the individual's interest in not being monitored.

The Administrative Court of Appeal has ruled that the disclosure of email addresses of the guardians of infants in an independent school was not permitted as it would be in breach of both the MPA and the PDA. The addresses were supposedly being used for marketing purposes. In this particular case the guardians had not been informed that their addresses could be disclosed to a third party and the Administrative Court of Appeal found that it therefore had to be assumed that the guardians wanted to keep their addresses private. The request to obtain the addresses was therefore rejected.

Switzerland

Lenz & Staehelin Dr Lukas Morscher & Martin Vonaesch

1. LEGISLATION

1.1 Name/title of the law

In Switzerland, the collection and processing of personal data is regulated by the Federal Act on Data Protection of 19 June 1992, as amended (DPA) and the Federal Ordinance on Data Protection of 14 June 1993, as amended (DPO).

In addition, several other laws contain provisions on data protection, especially laws which apply in regulated industries (such as financial markets and telecommunications), which further address the collection and processing of personal data:

- The Swiss Federal Code of Obligations (Code of Obligations) sets forth restrictions on the processing of employee data, and Ordinance 3 to the Swiss Federal Employment Act (Employment Act) limits the use of surveillance and control systems by the employer.
- The Swiss Federal Telecommunication Act (Telecommunication Act) regulates the use of cookies.
- The Swiss Federal Unfair Competition Act regulates unsolicited mass advertising by means of electronic communications such as e-mail and text messages ('spam').
- Statutory secrecy obligations, such as the banking secrecy (set forth in the Swiss Federal Banking Act (Banking Act)), the securities dealer secrecy (set forth in the Swiss Federal Stock Exchange and Securities Dealer Act (Stock Exchange Act) and the telecommunications secrecy (set forth in the Telecommunication Act), apply in addition to the DPA.
- The Banking Act, the Stock Exchange Act and the Swiss Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector (Anti-Money Laundering Act) stipulate specific duties to disclose information.

1.2 Pending legislation

The current versions of the DPA and the DPO were fully revised and amended in 2006/07 and entered into force on 1 January 2008. Currently, there is no pending legislation which would lead to a substantive change in Swiss data protection law.

1.3 Scope of the law

1.3.1 The main players

- The 'data processor' is not defined in the DPA. Anyone, whether private person or federal body, processing personal data of individuals or

legal entities is subject to the provisions in the DPA and the DPO. The answers in this questionnaire are generally limited to the processing of personal data by private persons.

- The 'owner of a data collection' is a private person or federal body that decides on the purpose and content of a data collection. A 'data collection' is a set of personal data the structure of which facilitates a search for data on a particular data subject.
- The 'data subject' is a natural person (individual) or legal entity whose data are processed.

1.3.2 Types of data

'Personal data' are defined as all information relating to an identified or identifiable person (individual or legal entity). A person is identifiable if a third party having access to the data on the person is able to identify such person with reasonable efforts.

In addition, the DPA lists 'sensitive personal data' and 'personality profiles' as special categories of personal data that are subject to stricter processing conditions.

'Sensitive personal data' are data on:

(i) religious, ideological, political or trade union-related views or activities;
(ii) health, the intimate sphere or the racial origin;
(iii) social security measures;
(iv) administrative or criminal proceedings and sanctions.

A 'personality profile' is a collection of data that permits an assessment of essential characteristics of the personality of a natural person.

1.3.3 Types of acts/operations

The DPA applies to any processing of personal data. 'Processing' is defined in the DPA as any operation with personal data irrespective of the means applied and the procedure. In particular, processing includes the collection, storage, use, revision, disclosure, archiving or destruction of personal data.

1.3.4 Exceptions

The DPA does not apply to:

- anonymised data;
- personal data that are processed by a natural person exclusively for personal use and are not disclosed to third parties;
- deliberations of the Federal Parliament and Parliamentary Committees;
- pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or administrative law, with the exception of administrative proceedings of first instance;
- public registers based on private law;
- personal data processed by the International Committee of the Red Cross.

1.3.5 Geographical scope of application

The DPA applies to any data processing that occurs within Switzerland. In addition, if a Swiss court decides on a violation of privacy by the media or other means of public information (eg the internet), the DPA may apply (even if the violating data processing occurred outside of Switzerland) if the data subject whose privacy was violated chooses Swiss law to be applied. Swiss law may be chosen as the applicable law if:

- the data subject has his usual place of residence in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland);
- the privacy violator has a business establishment or usual place of residence in Switzerland; or
- the result of the violation of privacy occurs in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland).

1.4 Particularities

The DPA generally applies not only to the processing of personal data of individuals, but also to the processing of personal data of legal entities. In addition, personality profiles (see the definition in section 1.3.2) are granted the same protection as sensitive personal data. Switzerland has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the EU.

2. DATA PROTECTION AUTHORITY

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (Federal Data Protection and Information Commissioner (FDPIC))
Feldeggweg 1, CH-3003 Bern, Switzerland
T: +41(0) 31 322 43 95
F: +41(0) 31 325 99 96
Web: *www.edoeb.admin.ch*

2.1 Role and tasks

The FDPIC is the federal data protection authority. He is appointed by the Federal Council for a term of office of four years. The FDPIC fulfils his tasks independently without being subject to the directives of any authority. He investigates cases in more detail on his own initiative or at the request of a third party if methods of processing are capable of violating the privacy of a large number of persons (system errors), if data collections must be registered (see section 6.2) or if there is a duty to provide information (see section 4). On the basis of his investigations the FDPIC may recommend that the methods of processing be changed. If a recommendation is not complied with or is rejected, the FDPIC may refer to the Federal Administrative Court for a decision (see also section 10.1)

Further the FDPIC provides assistance related to data protection and supervises private and federal bodies. He is responsible for the cooperation with data protection authorities in Switzerland and abroad. The FDPIC also maintains and publishes the register of data collections (see section 6.4).

2.2 Powers

The FDPIC has mostly investigative powers. He may issue recommendations in certain cases and, if such recommendations are not complied with or rejected, refer to the Federal Administrative Court for a decision (see section 2.1). However the FDPIC has no direct enforcement or sanctioning powers (see section 10.1).

2.3 Priorities

In 2010 and 2011 the FDPIC's practice focused on:

- internet and telecommunication (cookies, social media, cloud computing, online marketing);
- health insurance (patient records);
- smart meters (smart meters are electronic meters enabling consumption data for electricity to be recorded and automatically read and processed by energy suppliers);
- monitoring of employees;
- video surveillance by private persons.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Consent is not defined in the DPA. Pursuant to general principles of Swiss law, consent may be defined as the data subject's informed agreement to the processing of his personal data. If the general principles of data processing set forth in the DPA are complied with, no consent is required from the data subject to process his personal data. If the consent of the data subject is required for the processing of his personal data, such consent is valid only if given voluntarily based on adequate information. Furthermore, if such data to be processed are sensitive personal data or personality profiles, consent must be explicit.

3.1.2 Form

The DPA does not require that consent has to be given in writing by the data subject, even if explicit consent is required. Hence oral consent or electronic consent (eg by mouse click) is generally sufficient. For evidentiary purposes it is, however, generally advisable to obtain the data subject's consent explicitly and in recordable form. According to general principles, the data subject can withdraw his consent at any time. Further, the data subject generally does not have to react to requests from third parties. Therefore the mere fact that the data subject does not react to correspondence stating that the data subject's consent is deemed to be granted in case of non-reaction within a given period of time does not inevitably qualify as implied consent to a particular processing of data. However, this approach may be a valid and efficient course of action in the case of pre-existing relationships, if consent has to be obtained from many data subjects.

3.1.3 In an employment relationship

The data subject's consent is not a valid justification in an employment context, because pursuant to Article 328b Code of Obligations the employer may process data belonging to the employee only to the extent that such data relate to the employee's suitability for the employment relationship or are necessary to fulfil the employment contract. Since Article 328b Code of Obligations is of mandatory nature, employees cannot validly consent to any other (not employment relationship related) processing of their personal data (see also section 3.6.2 on monitoring of employees).

3.2 Other legal grounds for data processing

The DPA requires that personal data are always processed in accordance with the following principles:

- personal data may only be processed lawfully;
- the processing must be carried out in good faith and must be proportionate;
- the collection of personal data and in particular the purpose of their processing must be evident to the data subject;
- personal data may only be processed for the purpose indicated at the time of collection, which is evident from the circumstances, or which is provided for by law;
- anyone who processes personal data must make certain they are accurate (see section 3.4);
- personal data must be protected against unauthorised processing through adequate technical and organisational measures (see section 9);
- personal data must not be transferred outside of Switzerland if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection (see section 8);
- absent sufficient justification, sensitive personal data or personality profiles must not be disclosed to third parties;
- absent sufficient justification, personal data must not be processed against the explicit will of the data subject.

If the above principles are complied with, processing of personal data is generally considered lawful. Non-compliance with such principles constitutes a violation of the data subject's privacy unless the processing is justified by:

- the data subject's consent (see section 3.1);
- the law (eg, duty to disclose information as required under the Banking Act, the Stock Exchange Act, or the Anti-Money Laundering Act);
- an overriding private or public interest.

Pursuant to the DPA, an overriding interest of the person processing the data can in particular be considered if that person:

- processes personal data directly related to the conclusion or the performance of a contract and the personal data are those of the contractual party;
- processes personal data about competitors without disclosing them to third parties;
- processes personal data that are neither sensitive personal data

nor a personality profile (see section 1.3.) in order to verify the creditworthiness of the data subject provided that such data are only disclosed to third parties if they are required for the conclusion or the performance of a contract with the data subject;
- processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;
- processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning statistic etc, provided that the results are published in such a manner that the data subject may not be identified;
- collects personal data on a person of public interest, provided the data relate to the public activities of that person.

3.3 Direct marketing and cookies

In 2007, Switzerland adopted a full consent opt-in regime with respect to unsolicited mass advertisement by means of telecommunications (eg, email, SMS/MMS, fax or automated telephone calls). Pursuant to this law, the sender of an unsolicited electronic mass advertisement must seek the concerned recipient's prior consent to receive such mass advertisement and indicate in the advertisement the sender's correct contact information and a cost and problem free method to refuse further submissions. If a supplier collects customer data in connection with a sales transaction, the supplier may use such data for mass advertisement for similar products or services if the customer has been given the option to refuse such advertisement (opt-out) at the time of sale. The law does not specify for how long the supplier may use such customer data obtained through a sales transaction for mass advertisement. A period of about one year from the time of sale seems adequate.

The use of cookies is generally permissible, provided that the operator of the website (or other online service), which installs the cookie on the user's computer (or other device) informs the user about: (i) the use of cookies; (ii) the purpose of the use; and (iii) the user's right to refuse cookies.

3.4 Data quality requirements

Anyone who processes personal data must make certain the data are accurate. The data processor must take all reasonable measures to ensure that data which in view of the purpose of their collection are or have become incorrect or incomplete are either corrected or destroyed.

3.5 Outsourcing

The processing of personal data may be transferred to a third party if: (i) the transferor ensures that the third party will only process data in a way that the transferor is itself entitled to; and (ii) if no statutory or contractual secrecy obligations prohibit the processing by third parties. The transferor must make sure that the third party will comply with the applicable data security standards.

Although this is not a statutory requirement, data processing should be

outsourced to third parties by written agreement only. Such agreement will typically require the third party to process the personal data solely for the purposes of, and only under the instructions of, the transferor.

Special rules may apply in regulated markets. Article 47 of the Banking Act on banking secrecy protects customer-related data from disclosure to third parties and applies to all banking institutions in Switzerland. Any disclosure of non-encrypted data to a supplier is only allowed with the express consent of each banking customer. Consent can be given under the bank's general terms of business if they are made an integral part of the contract between the bank and its customers. The Banking Act does not prohibit the transfer of encrypted data (where the supplier cannot identify individual customers). Circular 2008/7 relating to outsourcing issued by the Swiss Financial Market Supervisory Authority FINMA applies to banks and securities dealers organised under Swiss law, including Swiss branches of foreign banks and securities dealers which are subject to FINMA supervision.

Before outsourcing a significant business area, these institutions must comply with the detailed measures set out in the circular, including:

(i) mandatory information of bank customers affected by the outsourcing;
(ii) careful selection, instruction and control of the supplier;
(iii) conclusion of a written contract with the supplier setting out, among others, the supplier's obligation to comply with professional secrecy rules.

3.6 Email, internet and video monitoring

3.6.1 General rules

The monitoring of email and internet use as well as the use of surveillance cameras is subject to the general data protection rules (see sections 3.1 and 3.2). The FDPIC has issued (non-binding) guidelines which specify the general principles in the DPA (see section 3.2) with respect to video surveillance by private individuals.

The guidelines provide, *inter alia*, that:

(i) video surveillance may only be conducted if less privacy-intrusive measures (additional locks, alarm systems) prove insufficient or impractical;
(ii) the video camera must be positioned in a way that only essential images for the intended purpose are recorded;
(iii) a clearly visible notice must inform people about the video surveillance; and
(iv) the images recorded must be deleted as soon as possible (generally within 24 hours).

The Swiss Federal Criminal Code sets forth several criminal offences for violation of secrecy and privacy which in specific cases may also apply to the recording and monitoring of email and internet traffic as well as video monitoring.

The telecommunication secrecy stipulated in the Telecommunication Act requires providers of telecommunication services (including internet providers) to keep confidential, and not to disclose information on, the

telecommunications traffic of their customers.

3.6.2 Employment relationship

The provisions of the DPA apply to email, internet and video monitoring in employment relationships. In addition, the Code of Obligations sets out the employer's duty to protect the employee's personality. Among others, the employer's right to use data concerning his employees is limited as follows: The employer may use data of the employee only to the extent that such data relate to the employee's suitability for the employment relationship or are necessary to fulfil the employment contract.

Ordinance 3 to the Employment Act generally prohibits the use of monitoring and control systems that monitor the employees' (general) behaviour at the workplace. Permanent monitoring of the email and internet traffic of employees by their employer is only permitted on a non-identity (ie anonymised or pseudonymised) basis. However, in case of an abuse or suspicion of abuse, an identity-based monitoring is permitted as long as it is only carried out retrospectively. The employer must inform the employees of the possibility to monitor internet use and email traffic.

In principle, content scanning of (business and private) emails constitutes a violation of the prohibition of identity-based, permanent monitoring of (general) behaviour of (specific) employees. It is, however, less problematic if an employer uses computer programs for the scanning of outgoing emails for certain keywords if the monitoring is used for legitimate reasons and by means of an automated monitoring system. Irrespective of whether the employees are allowed to use the internet and email for private purposes, the employer may generally not take insight into or read private emails or analyse their content in any way. Emails marked as private are generally considered equal to private correspondence and enjoy the same comprehensive protection. It is controversial in Swiss legal doctrine whether it always amounts to a violation of an employee's personal rights when a third party opens private mail or reads private emails.

4. INFORMATION OBLIGATIONS

4.1 Who

As a general principle, the collection of personal data and in particular the purpose of their processing must be evident to the data subjects. As a result covert data collection is not allowed.

The owner of a data collection is obliged to inform the data subject of the collection of sensitive personal data or personality profiles. This duty to actively provide information also applies if the data are collected from third parties.

4.2 What

The owner of a data collection that intends to collect sensitive personal data or personality profiles must inform the data subject of at least of the following:

- the identity of the owner of the data collection;

- the purpose of the data processing;
- the categories of data recipients if a disclosure of personal data is planned.

There are certain exceptions to this duty to inform, eg, if providing the information would result in the violation of overriding interests of third parties, or if the data collection owner's own overriding interests justify not informing the data subject (the latter only if personal data are not shared with third parties).

If the personal data have not been obtained directly from the data subject, but rather from a third party, the owner of the data collection must nevertheless provide the information stated above, except if:

- the data subject has already been informed;
- storage or disclosure is expressly provided for by law;
- the provision of information is not possible at all, or only with disproportionate inconvenience or expense.

4.3 When

The data subject has to be informed before the data are collected. If the data are not collected from the data subject, the data subject must be informed at the latest when the data are stored or if the data are not stored, on their first disclosure.

4.4 How

The information does not have to be provided in a specific form. For evidentiary purposes, however, the information should be provided in writing or other recordable form.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Any data subject may request information from the owner of a data collection as to whether personal data concerning the data subject are being processed. If this is the case, the data subject has the right to be informed about:

- all available personal data in the data collection concerning the data subject, including available information on the source of the data;
- the purpose and, if applicable, the legal basis of the processing;
- categories of personal data processed;
- other parties involved with the data collection;
- the recipients of the personal data.

Non-compliance with the right of access can be fined (see section 10.4). The right of access cannot be waived. If the owner of a data collection has personal data processed by a third party, he remains under an obligation to provide information. The third party is obligated to provide information if he does not disclose the identity of the owner of a data collection or if the latter is not domiciled in Switzerland.

5.1.2 Exceptions

The owner of a data collection may refuse, restrict, or delay the provision of information if:

- a formal law so provides;
- it is required to protect the overriding interests of third parties;
- it is required to protect an overriding interest of the owner of the data collection, provided that the personal data are not shared with third parties.

5.1.3 Deadline

The information must be provided in writing within 30 days of receipt of the request. If it is not possible to provide the information within such time period, the owner of the data collection must inform the data subject of the time period during which the information will be provided.

5.1.4 Charges

The information must usually be provided free of charge. As an exception, the owner of the data collection may ask for an appropriate share of the costs incurred if:

- the data subject has already been provided with the requested information in the 12 months prior to the request and no legitimate interest in the repeated provision of information can be shown, whereby in particular a modification of the personal data without notice to the data subject constitutes a legitimate interest; or
- the provision of information entails an exceptionally large amount of work.

The share of the costs may not exceed CHF 300. The data subject must be notified of the share of the costs before the information is provided and may withdraw his request within 10 days.

5.2 Rectification

5.2.1 Right

Any data subject may request that his personal data which are not or no longer accurate be rectified. Further, if it is impossible to demonstrate whether personal data are accurate or inaccurate the data subject may also request the entry of a suitable remark to be added to the particular piece of information/data.

5.2.2 Exceptions

The owner of a data collection must generally comply with such requests. However, the same exceptions as for the right to access apply (see section 5.1.2).

5.2.3 Deadline

There are no specified deadlines, but the rectification should be performed within a reasonable period of time.

5.2.4 Charges

The rectification must be performed free of charge.

5.3 Erasure

5.3.1 Right
The data subject can request that his personal data be erased.

5.3.2 Exceptions
The owner of a data collection must generally comply with such requests. However, the same exceptions as for the right to access apply (see section 5.1.2).

5.3.3 Deadline
There are no specified deadlines, but the erasure should be performed within a reasonable period of time.

5.3.4 Charges
The erasure must be performed free of charge.

5.4 Blocking
Not applicable.

5.5 Objection
5.5.1 Right
Any data subject may object either to the processing of his personal data or the disclosure of his personal data to third parties. However, the data subject's personal data can be processed against the data subject's will if such processing is justified (see section 5.5.2).

5.5.2 Exceptions
The owner of a data collection must generally comply with such requests. However, the same exceptions as for the right to access apply (see section 5.1.2).

5.5.3 Deadline
There are no specified deadlines, but the owner of a data collection should comply with the objection request within a reasonable period of time.

5.5.4 Charges
Objection requests are free of charge.

5.6 Automated individual decisions
Swiss data protection law does not address automated individual decisions. The general rules of the DPA and the DPO apply.

5.7 Other rights
Swiss data protection law does not provide further rights to the data subject other than the ones specified in sections 5.1 to 5.5.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

The data processor that transfers personal data outside of Switzerland is under certain circumstances obligated to notify the FDPIC of the data protection safeguards put in place (this duty to notify is addressed in section 8).

The owner of a data collection that (i) regularly processes sensitive personal data or personality profiles, or (ii) regularly discloses personal data to third parties, has the obligation to register such data collection with the FDPIC.

6.1.2 What

The FDPIC has to be informed by the owner of the data collection about:

- the name and the address of the owner of the data collection;
- the name and complete designation of the data collection;
- the person against whom the right of access may be asserted;
- the purpose of the data collection;
- the categories of personal data processed;
- the categories of data recipients;
- the categories of persons participating in the data collection, ie third parties who are permitted to enter and modify data in the data collection.

6.1.3 Exceptions

The owner of a data collection is not required to register a data collection if:

- he processes personal data due to a statutory obligation;
- he uses the data exclusively for publication in the edited section of a periodically published medium and does not pass any data to third parties without prior information;
- he has designated a data protection officer (see section 7);
- he has acquired a data protection quality mark under a certification procedure (see section 9.4);
- it falls within a list of further exceptions by the Federal Council set out in the DPO, which list includes, among others:
  (i) data collections of suppliers or customers, provided they do not contain any sensitive personal data or personality profiles;
  (ii) collections of data that are used exclusively for research, planning and statistics purposes;
  (iii) accounting records.

6.1.4 When

The data collection has to be registered before it is created. The owner of the data collection has the obligation to keep the data collection registration up to date.

6.1.5 How

The registration can be carried out by providing the required information (see section 6.1.2.) to the FDPIC in a letter, or by completing the official

registration form accessible on the FDPIC's website. Generally there are no further documents that have to be submitted along with the letter or completed registration form. To date, data collection registrations cannot be performed online.

6.1.6 Notification fees

There are no fees charged for data collection registrations.

6.2 Authorisation requirements

The DPA does not provide for authorisation requirements. The duty to notify transfers of personal data outside of Switzerland, and the duty to register data collections (see section 6.1) are mere notification requirements.

6.3 Other registration requirements

The appointment of an independent data protection officer will only result in a release of the duty to register data collections if the FDPIC is notified of the appointment of a data protection officer (see section 7).

6.4 Register

There is no publicly accessible register of contractual safeguards or binding corporate rules notified to the FDPIC with respect to transfers of personal data outside of Switzerland (see section 8).

The database of data collections registered with the FDPIC (see section 6.1) is publicly available and can be accessed by anyone through the internet (*www.datareg.admin.ch*) free of charge. On request, the FDPIC also provides paper extracts free of charge.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The appointment of a data protection officer is not mandatory in Switzerland. However, the registration of data collections (see section 6.1) is not required if the owner of a data collection has appointed a data protection officer that independently monitors data protection compliance within the owner's business organisation and maintains a list of data collections.

The data protection officer must have the necessary knowledge of:

(i) Swiss data protection law and how it is applied in practice;
(ii) the information technology and technical standards applied by the owner of the data collection; and
(iii) the organisational structure of the owner of the data collection and particularities of the data processing performed by the owner of the data collection.

The appointment of a data protection officer will only result in a release of the duty to register data collections if the FDPIC is notified of the appointment of a data protection officer. A list of such business organisations who have appointed a data protection officer is publicly accessible on the FDPIC's website.

7.2 Tasks and powers

The data protection officer has two main duties.

The data protection officer audits the processing of personal data within the organisation and recommends corrective measures if he finds that the data protection regulations have been violated he must not only assess compliance of the data processing with the data protection requirements on specific occasions, but also periodically. The auditing involves an assessment of whether the processes and systems for data processing fulfil the data protection requirements, and whether these processes and systems are in fact enforced in practice. If the data protection officer takes note of a violation of data protection regulations, he must recommend corrective measures to the responsible persons within the organisation and advise them on how to avoid such violations in the future. The data protection officer does however not need to have direct instruction rights.

The data protection officer maintains a list of the data collections that would be subject to registration with the FDPIC. The list is to be kept updated. Unlike the data collections registered with the FDPIC, the internal data collections do not have to be maintained electronically nor must they be available online. However, they must be made available on request to the FDPIC and to the data subjects.

The data protection officer must:

(i) carry out his duties independently and without instructions from the owner of the data collections;
(ii) have the resources required to fulfil his duties; and
(iii) have access to all data collections and all data processing as well as to all information that he requires to fulfil his duties.

There is no particular protection against dismissal of the data protection officer. The data protection officer can be an employee of the data controller or a third person.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Personal data may only be transferred outside of Switzerland if the privacy of the data subject is not seriously endangered, in particular due to the absence of legislation that guarantees adequate protection in the jurisdiction where the receiving party resides. The FDPIC has published on its website a list of jurisdictions which provide adequate data protection (*www.edoeb.admin.ch/themen/00794/00827/index.html?lang=en*). The EEA countries and Andorra, the Faroe Islands, Guernsey, the Isle of Man, Jersey, Monaco, Canada, Argentina, Israel and New Zealand are generally considered to provide an adequate level of data protection as regards personal data of individuals (however, many do not with regard to personal data of legal entities), while the laws of all other jurisdictions (including the US) do not provide for adequate data protection.

8.2 Legal basis for international data transfers

In the absence of legislation that guarantees adequate protection, personal data may only be transferred outside of Switzerland if:

- sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad (see sections 8.2.1 and 8.2.3);
- the data subject has consented in the specific case;
- the processing is directly connected with the conclusion or the performance of a contract and the personal data are those of a contractual party;
- disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;
- the data subject has made the data generally accessible and has not expressly prohibited their processing;
- disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules (ie binding corporate rules) that ensure an adequate level of protection (see section 8.2.2).

If data are transferred outside of Switzerland to a jurisdiction which does not provide for adequate data protection based on safeguards that ensure adequate protection such as contractual clauses (see section 8.2.1) or Safe Harbour certification (see section 8.2.3) or binding corporate rules (see section 8.2.2), the FDPIC must be notified of such safeguards. Although the FDPIC may during a period of 30 days review the safeguards, the data transferor does not have to wait for the result of the FDPIC's review or obtain approval. Moreover, if personal data are transferred outside of Switzerland on the basis of safeguards that have been pre-approved by the FDPIC (see section 8.2.1 and 8.2.3), the FDPIC only has to be informed about the fact that such safeguards are the basis of the data transfers.

8.2.1 Data transfer agreements

Data transfer agreements or data transfer clauses are regularly used in practice. It is the responsibility of the data transferor to ensure that an agreement is concluded that sufficiently protects the rights of the data subjects. The data transferor is free to decide whether or not to make use of a standard form. The FDPIC provides a model data transfer agreement (owner to processor), which can be accessed on its website. The model data transfer agreement is directly based on Swiss law and reflects to a large extent the standard contractual clauses of the European Commission for data transfers. Furthermore, the FDPIC has pre-approved the European Commission's standard contractual clauses and the model contract of the Council of Europe as safeguards which provide adequate data protection, although it is unclear whether they must be adapted to also cover personal data of legal entities and the protection of personality profiles.

8.2.2 Binding corporate rules

An acceptable method for ensuring adequate data protection abroad are binding corporate rules that sufficiently ensure data protection in cross-border data flows within the same legal person or company or between legal persons or companies that are under the same management. The owner of the data collection must notify the binding corporate rules to the FDPIC (see section 8.2 paragraph 2). Binding corporate rules should address at a minimum the elements covered by the model data transfer agreement provided by the FDPIC (see section 8.2.1.)

8.2.3 Safe Harbour

The US-Swiss Safe Harbour Framework (was established in 2009 to specifically address the Swiss data protection law particularities not covered by the US-EU Safe Harbour (ie, protection of personal data of legal entities and personality profiles)). Certification of US entities under the framework is considered by the FDPIC to be a safeguard that ensures adequate data protection and may therefore serve as the basis for a transfer of data to the certified recipient in the US. US firms can register and self-certify with the US Department of Commerce if they comply with the data protection principles contained in the 'US-Swiss Safe Harbour Framework'. These principles are:

(i) notice;
(ii) choice;
(iii) conditions for onward transfer;
(iv) security;
(v) data integrity;
(vi) access; and
(vii) enforcement.

In addition, they have to:

(i) publicly disclose their privacy policies;
(ii) accept jurisdiction of the US Federal Trade Commission or the US Department of Transportation; and
(iii) notify the US Department of Commerce of the self-certification.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Personal data that are subject to confidentiality obligations may generally only be processed in line with the respective confidentiality obligations. In particular, such personal data may not be processed by third parties (see also section 3.5).

The wilful and unauthorised disclosure of confidential, sensitive personal data or personality profiles which have come into the possession of the disclosing person in the course of his professional activities (where such activities require the knowledge of such data) is, on complaint, punishable by a fine of up to CHF10,000 (regarding sanctions see section 10.4).

9.2 Security requirements

Personal data must be protected by appropriate technical and organisational measures against unauthorised processing. Anyone processing personal data

or providing a data communication network must ensure the confidentiality, availability and the integrity of the data. In particular the personal data must be protected against the following risks:

- unauthorised or accidental destruction;
- accidental loss;
- technical faults;
- forgery, theft or unlawful use;
- unauthorised alteration, copying, access or other unauthorised processing.

The technical and organisational measures must be adequate and must be reviewed periodically. In particular, the following criteria must be taken into account:

- the purpose of the data processing;
- the nature and extent of data processing;
- an assessment of the possible risks to the data subjects;
- the current state of the art (especially currently available technology).

In relation to automated data processing the owner of the data collection must take the appropriate technical and organisational measures to achieve, in particular, the following goals:

- data access control: unauthorised persons must be denied access to facilities in which personal data are being processed;
- personal data carrier control: preventing unauthorised persons from reading, copying, altering or removing data carriers;
- transport control;
- disclosure control: data recipients to whom personal data are disclosed by means of devices for data transmission must be identifiable;
- storage control;
- access control: the access by authorised persons must be limited to the personal data that they require to fulfil their task;
- input control: in automated systems, it must be possible to carry out a retrospective examination of what personal data were entered at what time and by which person.

9.3 Data security breach notification obligation

Swiss data protection law does not know a general data security breach notification obligation. As a rule, it would contravene general principles of tort law to provide for an obligation of the violator to proactively inform the damaged person(s). Nevertheless, it is currently discussed whether such rules on data security breach notifications shall be implemented in Swiss law on an autonomous basis.

9.4 Data protection impact assessments and audits

With regard to audits by an appointed data protection officer, see section 7.2 above. The DPA provides for a certification procedure by recognised independent certification organisations. The manufacturers of data processing systems or programs as well as private persons that process personal data may submit their systems, procedures and organisation for

evaluation to those certification organisations. Although registration of data collections is not required if the owner of the data collection has acquired a data protection quality mark under such a certification procedure (see section 6.2), the certification procedure has remained largely irrelevant in practice due to the fact that the same advantages are achieved by appointing a data protection officer (see section 7).

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The FDPIC has no direct enforcement powers against private bodies processing personal data. Nevertheless the FDPIC can carry out investigations if methods of processing are capable of violating the privacy of a large number of persons (system errors), if data collections must be registered (see section 6.1) or if there is a duty to provide information (see section 4). To this effect the FDPIC may request documents, make inquiries and attend data processing demonstrations. On the basis of his investigations, the FDPIC may recommend that a certain method of data processing be changed or abandoned. However these recommendations are not binding, but if a recommendation made by the FDPIC is not complied with or is rejected, he may refer the matter to the Federal Administrative Court for a decision. The FDPIC has the right to appeal against such decision to the Federal Supreme Court.

10.2 Sanctions

Non-compliance with recommendations of the FDPIC is not criminally sanctioned because the recommendations of the FDPIC are not binding. Likewise violations of the data protection principles (see section 3.2) are generally not criminally sanctioned. However private persons are liable to a fine up to CHF 10,000 if they wilfully:

- fail to provide information with regard to safeguards in case of cross-border disclosures (see section 8) or to declare data collections (see section 6.1) or in so doing wilfully provide false information; or
- provide the FDPIC with false information in the course of an investigation, or refuse to cooperate.

Further criminal sanctions may apply on a private person's complaint (see section 10.4).

10.3 Examples of recent enforcement of data protection rules

See section 10.7.

10.4 Judicial remedies

Violations of the DPA may be asserted by the data subject in a civil action against the violator. The data subject may, in particular, request that the data processing be stopped, that no personal data be disclosed to third parties or that the personal data be corrected or destroyed (regarding the rights of rectification and objection see sections 5.1-5.5). Moreover the data subject can seek assistance of the court in enforcing his right to access (see section 5.1).

Further the data subject may file claims for damages and reparation for moral damages (*Genugtuung*) or for the surrender of profits based on the violation of his privacy, and may request that the rectification or destruction of the personal data or the judgment be notified to third parties or be published.

In addition, certain actions or inactions by private persons may, on complaint, be criminally investigated and result in criminal sanctions. The intentional non-compliance with the following duties are punishable by a fine of up to CHF 10,000:

- the data subject's right of access (see section 5.1) by refusing to allow access or by providing wrong or incomplete information;
- the duty to inform the data subject on the collection of sensitive personal data or personality profiles (see section 4.1);
- the duty of confidentiality of certain professionals to keep sensitive personal data and personality profiles (see section 9.1).

10.5 Class actions

Swiss law does not have class actions.

10.6 Liability

Generally, see section 10.4.

The FDPIC filed suit against Google in connection with Google's Street View service after Google had decided not to accept the FDPIC's recommendations with respect to the company's practice on anonymising faces of people and number plates of cars that are captured on the Street View photographs published on the internet (the automatic system is technically incapable of blurring all faces and number plates). In March 2011 the Federal Administrative Court (FAC) decided in favour of the FDPIC and held that all faces and number plates must be made unrecognisable before the images are published on Google Street View and made accessible on the internet. In its ruling the FAC in particular concluded that the public interest in having a visual record of all streets and Google's commercial interests could not outweigh the affected individuals' rights in their own image. Google has appealed the FAC's decision with the Federal Supreme Court (FSC) where the case is currently pending.

In the case *FDPIC v Logistep* the Federal Supreme Court in September 2010 held that IP addresses may under certain circumstances qualify as personal data. Logistep provides services to copyright owners to identify copyright law infringers in peer-to-peer networks. The FSC held that Logistep's actions contravened the data protection principles set forth in the DPA, specifically due to the fact that the (hidden) collection of the peer-to-peer network's users' IP addresses was not recognisable to such users. The FSC concluded that this violation of the data protection principles in the given case cannot be justified by overriding public or private interests of the copyright owners. The FDPIC had appealed the FAC's previous decision which concluded that the interests of the copyright owners outweigh the peer-to-peer network users' data protection interests.

Turkey

ELİ G Attorneys at Law Gönenç Gürkaynak, Ilay Yılmaz & Ceren Yıldız

1. LEGISLATION

1.1 Name/title of the law

Turkey has no specific fully-fledged law governing the privacy of personal data. The applicable legislation in this respect is:

- Articles 20 and 22 of the Turkish Constitution of 1982, which generally protect privacy of personal life and communication, respectively;
- Article 24 of the Turkish Civil Code, which entitles individuals whose personal rights are unjustly violated to file a civil action; and
- Articles 135, 136 and 138 of the Turkish Criminal Code, which regulate unlawful storage of, transmission or reception of, and failure to destroy personal data, respectively.

1.2 Pending legislation

There is a draft law on the protection of personal data (Draft Law), which has been submitted to the General Assembly of the Turkish law-making parliament for ratification, however, no progress has been made since the Draft Law was put on the agenda in 2006 and the Draft Law is declared as being void in the Turkish parliament's online records.

1.3 Scope of the law

1.3.1 The main players

Due to the lack of a comprehensive law on the issue, the players are not explicitly defined under the legislation. Having said that, the Turkish Criminal Code imposes sanctions on persons who unjustly: (i) record or (ii) acquire or disseminate personal data, or give personal data to third persons.

1.3.2 Types of data

The Turkish Civil Code does not provide a comprehensive list in respect of personal rights and leaves the matter to the discretion of the judge. Therefore, the question of whether the data that will be collected qualify as a personal right within the meaning of Article 24 of the Turkish Civil Code will depend on the judicial precedents on the matter. In this respect, the relevant jurisprudence and the scholarly writings give weight to the will of the data owner, ie, the fact of whether the data owner considers the collected data to be personal.

Unlike the Turkish Civil Code, the Turkish Criminal Code adopts a definition of 'personal data', which does not fall far from the definition provided in the Council of Europe's Convention of 28 January 1981 for the

Protection of Individuals with regard to Automatic Processing of Personal Data. On this basis, the rationale of the Turkish Criminal Code makes reference to the penal code of France and states that '*information relating to and sufficient enough to identify an individual*' would qualify as 'personal data' within the meaning of Article 9 of the Turkish Criminal Code. Nevertheless, the question of whether any given data would qualify as 'personal data' will ultimately be assessed by the criminal judge on a case-by-case basis.

1.3.3 Types of acts/operations

Article 20 of the Turkish Constitution of 1982 regulates the act of processing – without any definitions – and states that personal data may only be processed in cases where it is stipulated by law or with the owner's explicit consent.

Article 22 of the Turkish Constitution of 1982 regulates the privacy of communication and states that communication cannot be hindered and its privacy cannot be violated.

Article 24 of the Turkish Civil Code addresses 'violation' and entitles individuals whose personal rights are unjustly violated to file a civil action. The Turkish Criminal Code regulates the acts of:

(i) unlawful storage of personal data;
(ii) unlawful transmission or reception of personal data; and
(iii) failure to destroy any personal data even after the waiting periods set forth in the law have passed.

The Turkish Criminal Code addresses the unlawful storage of, transmission or reception of, and failure to destroy personal data. However, the Turkish Criminal Code (or any other statute) does not define the phrase 'unlawful'. The term unlawful in this context may be interpreted as storage or transmission of personal data without consent from the relevant individuals.

1.3.4 Exceptions

Article 24 of the Turkish Civil Code stipulates that all violations addressed to personal rights are deemed unlawful except where:

(i) the person whose rights are violated gives his/her consent;
(ii) there is a higher private or public benefit; or
(iii) authorisation which has arisen from law is exercised.

1.3.5 Geographical scope of application

The legislation currently in force applies to the territory of Turkey.

1.3.6 Particularities

As per the Turkish Criminal Code, if the person who unlawfully stores, transmits or receives personal data is a public officer and is committing these crimes by misusing its public authority, or benefits the facilities of a particular profession and art, the punishment shall be increased by 50 per cent.

2. DATA PROTECTION AUTHORITY

There is no specific data protection authority in Turkey.

Pursuant to Article 24 of the Turkish Civil Code, an individual whose personal rights are violated unjustly is entitled to file a civil action before the general courts.

As per Article 139 of the Turkish Criminal Code, the data privacy crimes stipulated thereunder are *ex officio* investigated by the public prosecutor and are not subject to complaint by the injured party. In this respect, Turkish public prosecutors and courts are authorised to protect data privacy.

2.1 Role and tasks

Not applicable.

2.2 Powers

Turkish courts are authorised to impose criminal and legal sanctions.

2.3 Priorities

Not applicable.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Article 20 of the Turkish Constitution of 1982 states that personal data may be processed with the owner's explicit consent. 'Consent' regarding data privacy is not defined in any relevant legislation or case law.

By virtue of Article 24/II of the Turkish Civil Code, prior consent of the data owner is considered to be a legitimising factor.

The term 'unlawful' in Articles 135 and 136 of the Turkish Criminal Code may be interpreted to mean lack of consent from the relevant individuals for storage, transmission or receipt of the personal data.

3.1.2 Form

Not applicable.

3.1.3 In an employment relationship

The Turkish Employment Law provides that the employer is obliged to use the personal data of its employees in accordance with the law and the principle of good faith.

3.2 Other legal grounds for data processing

Other legal grounds include cases where there is a higher private or public benefit or authorisation which has arisen from law is exercised.

3.3 Direct marketing and cookies

Not applicable.

3.4 Data quality requirements

Not applicable.

3.5 Outsourcing
Not applicable.

3.6 Email, internet and video monitoring
3.6.1 General rules
Not applicable.

3.6.2 Employment relationship
Personal data should be used in accordance with the laws and the principle of good faith. There are no legal obstacles against the employee granting consent to his/her employer for the use of its personal data.

4. INFORMATION OBLIGATIONS
There is no obligation to provide any information to data subjects in Turkey.

5. RIGHTS OF INDIVIDUALS
5.1 Access
5.1.1 Right
Under Article 20 of the Turkish Constitution of 1982, everyone has the right to request the protection of their personal data. This right covers providing information to the relevant person about their personal data; access to their personal data; the right to request the rectification or erasure of their personal data; or the right to know whether their data are being used lawfully and in accordance with proper purposes.

5.1.2 Exceptions
Not applicable.

5.1.3 Deadline
Not applicable.

5.1.4 Charges
Not applicable.

5.2 Rectification
5.2.1 Right
Article 20 of the Turkish Constitution of 1982 provides the right to request the rectification of incorrect personal data.

5.2.2 Exceptions
Not applicable.

5.2.3 Deadline
Not applicable.

5.2.4 Charges

Not applicable.

5.3 Erasure

5.3.1 Right

Article 20 of the Turkish Constitution of 1982 provides the right to request the erasure of personal data.

5.3.2 Exceptions

Not applicable.

5.3.3 Deadline

Not applicable.

5.3.4 Charges

Not applicable.

5.4 Blocking

Not applicable.

5.5 Objection

Not applicable.

5.6 Automated individual decisions

Not applicable.

5.7 Other rights

5.7.1 Right

Article 20 of the Turkish Constitution of 1982 provides the right to find out if personal data are being used in accordance with proper purposes.

5.7.2 Exceptions

Not applicable.

5.7.3 Deadline

Not applicable.

5.7.4 Charges

Not applicable.

6. REGISTRATION OBLIGATIONS

Not applicable.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

It is not mandatory to appoint a data protection officer and this role is not recognised by law.

Appointing data protection officers in organisations is not very common

in Turkey.

7.2 Tasks and powers
Not applicable.

8. INTERNATIONAL DATA TRANSFERS
8.1 Applicable rules
Article 136 of the Turkish Criminal Code, without making a distinction between international and domestic data transfers, states that anyone who unlawfully transfers personal data shall be sentenced.

8.2 Legal basis for international data transfers
Not applicable.

9. SECURITY OF DATA PROCESSING
There is no specific obligation with regard to the confidentiality or the security of personal data in the data protection provisions. The general provisions, ie Articles 20 and 22 of the Turkish Constitution of 1982, Article 24 of the Turkish Civil Code, and Articles 135, 136 and 138 of the Turkish Criminal Code, as stipulated above apply.

9.1 Confidentiality
Not applicable.

9.2 Security requirements
Not applicable.

9.3 Data security breach notification obligation
There exists no obligation to notify individuals or any authority about any data breaches. Such notifications are not common in practice in Turkey. However, under general provisions that apply to personal data, anyone whose rights with respect to his/her personal data are breached, might sue the breaching party or might notify the suspect to the competent authorities for criminal investigation if the breach constitutes a crime.

9.4 Data protection impact assessments and audits
Not applicable.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY
10.1 Enforcement actions
As per Article 139 of the Turkish Criminal Code, the data privacy crimes stipulated under the Turkish Criminal Code are *ex officio* investigated by the public prosecutor.

In this respect, public prosecutors and consequently courts can take enforcement actions.

10.2 Sanctions

Sanctions under the Turkish Criminal Code include:

- Article 135/I: Unlawful storage of personal data may trigger imprisonment from six months to three years.
- Article 136/I: In the case of unlawful transmission or receipt of personal data, the penalty is increased to imprisonment from one year to four years.
- Article 138: Any person who fails to destroy any personal data, even after the waiting periods set forth in the law have passed, may face imprisonment from six months to one year. If such crimes are committed by a legal entity, the entity will be subject to the security measures set forth under Article 60 of the Turkish Criminal Code. Such security measures are, as the case may be: (i) if the entity carries out its commercial activities by virtue of a permit granted by a public institution, cancellation of such permit of activity; and (ii) seizure of the relevant goods and objects that were used in committing the crime.

There are no administrative offences and penalties stipulated by law, however, persons whose personal rights are violated might apply to general courts and request pecuniary and non-pecuniary damages.

10.3 Examples of recent enforcement of data protection rules

We are not aware of any precedents regarding the enforcement of the foregoing rules.

10.4 Judicial remedies

Pursuant to Article 24 of the Turkish Civil Code, an individual whose personal rights are violated unjustly is entitled to file a civil action before the general courts. Personal rights capture the personal data as well.

Courts are entitled to stop the distribution, publication etc of any personal data which are used without the owner's permission and/or against the law. For example, in a precedent of the Supreme Court Assembly of Chambers (2001/4-926E and 2001/742K) dated 17 October 2001, a photograph of a person was published without permission, and the court of first instance decided to stop the publication and distribution of the photograph as injunctive relief.

10.5 Class actions

Not applicable.

10.6 Liability

Individuals can claim damages before the general courts. The precedents in general capture the privacy of communication and private life.

In one instance of the Supreme Court for the 4th Circuit (2009/8119E, 2010/7573K) dated 23 June 2010, whereby the correspondence between two persons was secretly recorded, the court decided that the audio record was obtained against the law and that secrecy and recording of audio in a secret manner constitutes a violation of personal rights and that the defendant

should pay a certain amount of compensation for non-pecuniary damages. However, the amount of compensation was not indicated in the decision.

In another instance, the Supreme Court for the 4th Circuit (2009/14515E, 2011/1353K) dated 16 February 2011, the court granted non-pecuniary damages to the plaintiff, whose private phone conversations were disclosed. There is no information as to the amount of compensation awarded.

United Kingdom

Bristows Hazel Grant & Mark Watts

1. LEGISLATION

1.1 Name/title of the law

In the UK the law implementing the Directive is entitled the Data Protection Act 1998 (the DPA).

The implementing law of the ePrivacy Directives (2009/136/EC and 2002/58/EC) is the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

1.2 Pending legislation

There is no pending legislation that would materially affect the DPA.

1.3 Scope of the law

1.3.1 The main players

In UK data protection law the main players are as follows:

- 'Data controller' means a person who determines the purposes for which and the manner in which any personal data are or are to be processed. It is possible for a data controller to make this determination either alone or jointly or in common with other persons.
- 'Data processor' means a person other than an employee of the data controller who processes data on behalf of a data controller.
- 'Data subject' means an individual who is the subject of personal data.

1.3.2 Types of data

Other key definitions include:

- 'Personal data' means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of or likely to come into possession of the data controller. The term includes any expression of opinion about an individual and any indication of the intentions of that data controller or any other person in respect of the individual. In the UK there has been case law considering this definition, in particular see *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746. This case held that to be personal data the information concerned must: (i) be 'biographical in a significant sense'; and (ii) 'focus' on the individual, rather than some other person or transaction or event. This has led to a view that the UK courts interpret the definition of personal data very narrowly, and therefore differently from the view held in mainland European jurisdictions (and the view of pan-European advisory bodies such as the Article 29 Working Party). The UK data protection authority has issued

guidance on this definition that attempts to harmonise UK case law and European guidance. In practice however it is possible that a case heard before the UK courts that turned on the definition of personal data might have a different result to a complaint based on the same circumstances being considered by the UK data protection regulator;

- 'Sensitive data' means the following types of information: racial or ethnic origin of the data subject; political opinions; religious beliefs or beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; commission or alleged commission of any offence; any proceedings for any offence committed or alleged to have been committed by the individual, including the sentence of any court in any such proceedings.

The DPA does not protect corporate information: however in some limited circumstances marketing to corporates is restricted under direct marketing legislation referred to in section 3 below.

1.3.3 Types of acts/operations

The DPA broadly defines 'processing' to include obtaining, recording or holding information together with carrying out any operation or set of operations on the information including organisation, adaptation, alteration, retrieval, consultation, use, disclosure, alignment, combination, blocking, erasure or destruction.

The DPA governs both automated and manual processing. Manual processing is covered by the DPA if it falls within the definition of a 'relevant filing system'. The definition of a 'relevant filing system' means any set of information relating to individuals to the extent that the set is structured either by reference to individuals or by reference to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible.

UK case law has interpreted this definition very narrowly to the extent that, in effect, only highly organised paper filing systems (close to the level of organisation in a computerised system) would fall within this definition.

1.3.4 Exceptions

The UK has chosen to apply the DPA to personal data processed for security, defence and criminal law. Within the DPA there are specific exemptions the effects of which are to remove some of the obligations under the DPA in relation to the processing of information held for security, defence and police matters.

Personal data processed by a natural person in the course of purely personal or household activity is exempted under the DPA.

1.3.5 Geographical scope of application

The DPA applies to a data controller who is either:

- established in the UK where the data are processed in the context of that establishment; or

- established in neither the UK nor in any other EEA state but uses equipment in the UK for the processing of data otherwise than for the purposes of transit through the UK.

Where a data controller uses equipment within the UK it must nominate a representative established in the UK.

Establishment includes individuals ordinarily resident in the UK, corporate bodies incorporated in the UK, partnerships or other unincorporated associations formed under UK law and legal persons who maintain in the UK an office, branch agency or regular practice.

1.4 Particularities

None.

2. DATA PROTECTION AUTHORITY

Information Commissioner's Office
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF
United Kingdom
T: 01625 545745
F: 01625 524510
E: pressoffice@ico.gsi.gov.uk
W: *www.ico.gov.uk*

2.1 Role and tasks

The Information Commissioner is considered to be a corporation sole and both he and his officers and staff are not considered servants or agents of the UK crown (unlike most other government employees within the UK). The UK regulator is often referred to as the ICO.

Broadly the ICO's role and responsibilities include:

- maintaining a register of data controllers;
- issuing guidance and promoting good practice in data protection compliance; and
- investigating complaints and carrying out enforcement in situations involving breaches of the DPA.

Additionally, the ICO is responsible for freedom of information enforcement within England, Wales and Northern Ireland.

2.2 Powers

The ICO has the following powers:

- Information notices: the ICO can require the delivery of information to the Commissioner to enable him to carry out investigations.
- Powers of entry and inspection: the ICO can enter premises and carry out inspections on site, however he requires a warrant from court to do so.
- Enforcement notices: an enforcement notice is, in effect, an order issued by the ICO requiring a data controller to rectify its practices. The notice is made public and breach of the notice would be contempt of court.

- Audit: the ICO can require central government departments to submit to

an audit of data protection compliance. This power has been confirmed by Prime Ministerial order to central government departments. As at the date of writing, there is no similar obligation on local government, other government bodies or the private sector, however, the ICO is calling for an audit power to be available to him in the wider public sector and the private sector.

- Monetary penalties: The ICO is entitled to serve a monetary penalty notice (ie fine) of up to £500,000 for a serious contravention of the data protection principles under the DPA which is likely to cause substantial damage or distress. The contravention must be either: (i) deliberate; or (ii) in circumstances where the data controller knew or ought to have known that the contravention would occur and that it would be likely to cause substantial damage or distress but failed to take reasonable steps to prevent the contravention.

2.3 Priorities

The ICO's annual report for 2011 shows the following aims for the organisation:

- to improve the internal processes at the ICO and to integrate more closely the data protection and freedom of information compliance regimes;
- to reduce the numbers of times organisations get information rights wrong by being more proactive and imaginative in communicating with organisations on their responsibilities; and
- to use new data protection powers to undertake audits and impose civil monetary penalties.

3. LEGAL BASIS FOR DATA PROCESSING

3.4 Consent

3.4.1 Definition

There is no specific definition of consent within the UK's DPA.

The ICO has provided guidance (in the employment field and in relation to online data) which broadly follows the Article 29 Working Party view on the definition of consent.

3.4.2 Form

There is no requirement in the DPA for any particular form of consent. Similarly ICO guidance does not dictate any particular form of consent.

3.4.3 In an employment relationship

ICO guidance emphasises that it will be difficult to obtain freely given consent in an employment context. This point extends to applicants for jobs where the closer the individual is to becoming an employee the more difficult it is to obtain his or her freely given consent.

3.5 Other legal grounds for data processing

Any processing of any personal data requires a data controller to meet one of the following legal bases for processing:

- the data subject has given his consent for processing;
- the processing is necessary for the performance of a contract to which the data subject is party, or it is necessary for the taking of steps at the request of the data subject with a view to entering into a contract;
- the processing is necessary for compliance with any legal obligation to which the data controller is subject other than an obligation imposed by contract;
- the processing is necessary in order to protect the vital interests of the data subject;
- the processing is necessary for one of a number of governmental reasons such as: the administration of justice; the exercise of functions of either House of Parliament; the exercise of any functions conferred on any person by legislation; the exercise of functions of the Crown or a government department; or the exercise of other functions of a public nature exercised in the public interest by any person; and/or
- the processing is necessary for purposes of legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. Note that this legal basis for processing is widely used in the UK.

If sensitive data are being processed then, additionally, the data controller must meet one of the following legal bases for processing of sensitive data:

- the data subject has given his explicit consent for the processing of the data;
- the processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- the processing is necessary in order to protect the vital interests of the data subject or any other person in a case where consent cannot be given by the data subject or the data controller cannot reasonably be expected to obtain consent from the data subject or the data subject has unreasonably withheld his consent;
- the processing is carried out in the course of legitimate activities by a body or association which is not established or conducted for profit and exists for philosophical religious or trade union purposes. Such processing must be carried out with appropriate safeguards and relate only to members of the body or association or those who have regular contact with it and does not involve disclosure of personal data to a third party without consent of the data subject;
- the information has been made public as a result of deliberate steps taken by the data subject;
- the processing is necessary for the purpose of or in connection with any legal proceedings including prospective legal proceedings or is necessary for the purpose of obtaining legal advice or is otherwise necessary for the purpose of establishing, exercising or defending legal rights;

- the processing is necessary for a number of governmental reasons

including: the administration of justice; the exercise of any functions of either House of Parliament; the exercise of functions conferred on any person by legislation; or the exercise of any functions of the Crown, or a government department;

- the processing is necessary for medical purposes and is undertaken by a health professional or someone who owes a similar duty of confidentiality. In this case medical purposes includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services;
- the processing is of a racial or ethnic origin data and is necessary for equal opportunities monitoring and is carried out with appropriate safeguards for the rights and freedom of individuals;
- the processing is in the substantial public interest, is necessary for the purposes of the prevention or detection of any unlawful act, and must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes;
- the processing is in the substantial public interest, is necessary to protect members of the public against dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person and must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function;
- the processing is in the substantial public interest; is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and is carried out without the explicit consent of the data subject because the consent cannot be given by the data subject, the data controller cannot reasonably be expected to obtain the explicit consent of the data subject, or must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, advice, support or other service;
- the processing is necessary for the purpose of carrying on insurance business, or making determinations in connection with eligibility for, and benefits payable under, an occupational pension scheme and is of sensitive data consisting of information relating to a relative of an insured person or scheme member where the data controller cannot reasonably be expected to obtain the explicit consent of that data subject and the data controller is not aware of the data subject withholding his consent; and does not support measures or decisions with respect to that data subject.
- the processing is of sensitive data that is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons holding different beliefs or with different states of physical or mental health or different physical or mental conditions, and where such processing does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject and does not cause, nor is likely to cause, substantial damage or substantial distress to the data

subject or any other person;
- the processing is carried out by any recognised political party in the course of his or its legitimate political activities; and does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person;
- the processing is in the substantial public interest; is necessary for research purposes; does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person; and/or
- the processing is necessary for the exercise of any functions conferred on a constable (ie a policeman) by any rule of law.

The disclosure of information to a third party (other than potentially to a data processor) is considered to be processing and therefore would need to meet one of the legal bases as described above.

3.6 Direct marketing and cookies

Under the DPA there is a right for individuals to prevent marketing for direct marketing purposes (see below). This right together with obligations on transparency and the legal basis for processing (generally considered to be the legitimate interests of the marketer) has led to guidance from the ICO which can be summarised as follows:
- Dependent on the context it is usually possible for direct marketing to be sent by post to existing clients and/or those who have requested information on particular products or services. This is because it is considered to be within the individual's contemplation that further marketing will be sent on similar products or services.
- If an organisation intends to compile a list of direct marketing contacts and sell that list it would be necessary to inform the individuals and at the very least give them the option to opt out of receiving direct marketing from third parties.
- Direct marketing by email or SMS requires in general the prior consent of the individual. There is no requirement that this consent be provided by opt in, but the notice and opt in/opt out wording must be sufficiently clear to the individual.
- There is an exemption which allows direct marketing by email or SMS from an organisation to an existing client (so-called soft opt in).

There are some limited rules for corporates to permit the opting out of marketing calls. It is possible for individuals and corporates to notify the Fax Preference Service and the Telephone Preference Service to opt out of receiving direct marketing faxes and phone calls. Individuals can also opt out of receiving direct marketing by post through the Mail Preference Service. These preference services are enforced by the ICO under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004).

Rules on use of cookies previously required: (i) notification, generally carried out through a privacy policy; and (ii) ability to opt out, generally offered through browser settings.

These rules were updated in 2011 by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. The ICO has issued guidance on these new regulations and its interpretation. The ICO has required prior consent to the use of cookies and notified that use of browser settings is, at present, unacceptable. The ICO offered a number of different alternatives including use of pop-ups. However, due to the difficulty of finding a technical solution at present the ICO has agreed that it will not carry out any enforcement of these new cookie rules until May 2012. In the meantime, the ICO recommends that organisations using cookies should carry out an assessment of the cookies being used and plan how they will ensure compliance for May 2012.

3.7 Data quality requirements

Under the UK DPA there are eight data protection principles. These include a number of data quality requirements as follows:

- Third data protection principle: personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Fourth data protection principle: personal data shall be accurate and, where necessary, kept up to date.
- Fifth data protection principle: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

3.8 Outsourcing

Under the UK DPA the seventh data protection principle requires data controllers to ensure appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. This is then further interpreted in the DPA to include the following obligations:

- first, that a data controller must take reasonable steps to ensure the reliability of any employees of his who have access to personal data;
- second, to ensure where processing is carried out by a data processor on behalf of the data controller, the data processor chosen provides sufficient guarantees in respect of the technical and organisational security measures governing the processing and takes reasonable steps to ensure compliance with those measures; and
- third, when processing personal data using a data processor, that processing must be carried out under a contract which is made or evidenced in writing and under which the processor is to act on the instructions of the data controller and the data processor complies with security obligations equivalent to those imposed on a data controller by the seventh principle.

In practice, therefore, data controllers put in place contracts which include a data protection clause requiring, at the very least, that the data processor

acts on the instructions of the data controller and ensures adequate, technical and organisational measures to protect the personal data. Often the clauses are more complex and include obligations on vetting and monitoring of staff, assisting with investigations by the ICO and notifying and responding to data losses. Following on from enforcements by the ICO in situations where personal data have been compromised whilst being processed by a data processor, it seems likely that data processor contracts will increasingly include the right to audit data processor compliance.

3.9 Email, internet and video monitoring

3.9.1 General rules

There are no specific rules under the DPA relating to monitoring of email and internet usage or use of surveillance cameras. However the ICO has produced guidance on all of these topics. There are some additional rules in the Regulation of Investigatory Powers Act 2000 relating to interception of communications. This would apply in the case of monitoring email, internet usage and phone communications.

The DPA will apply where personal data are being recorded and this will depend on whether the individuals affected can be identified (eg CCTV cameras directed towards a crowd when there is no likelihood of identification might not be considered to be collecting personal data) and when the information is actually being recorded (eg listening into a telephone call without recording it or taking notes would not engage the DPA, however this would engage the Regulation of Investigatory Powers Act).

Use of video surveillance in general requires a privacy impact assessment to be carried out by the data controller to ensure that it is an appropriate use of the technology together with appropriate notices that CCTV cameras are in use and identifying the data controller of the camera, together with the purpose for which it is being used. Data quality requirements are particularly important in terms of the CCTV images.

Email, internet and phone monitoring would all require a privacy impact assessment to be carried out by the data controller to ensure that it is an appropriate method to achieve the purposes required. There would be a need for general notification that this was happening to the ICO and appropriate structures to deal with handling the information collected from the monitoring in a sensitive fashion.

3.9.2 Employment relationship

The ICO has produced guidance entitled the Employment Practices Code (this includes the guidance referred to above on monitoring employees and workers). Under this Code, employers are generally required to notify employees of the scope of monitoring carried out and its purposes. Providing an appropriate privacy impact assessment is carried out there is unlikely to be a requirement for consent to the monitoring of employees (although some employers still use consent mechanisms. The ICO does not approve of the use of consent in the employment relationship due to the likely difficulty for the employee to refuse consent).

Under the Regulation of Investigatory Powers Act an employer is permitted

to monitor communications on its network for a number of different purposes including, for example, to check that internal rules and practices are being observed.

4. INFORMATION OBLIGATIONS

4.1 Who

The information should be provided to the data subject concerned.

4.2 What

The information to be provided includes:

- the identity of the data controller or, if he has nominated a representative for the purposes of the DPA, the identity of that representative;
- the purpose or purposes for which the personal data are intended to be processed;
- any further information which is necessary having regard to the specific circumstances in which the data are or are to be processed to enable processing in respect of the data subject to be fair.

4.3 Exceptions

Where personal data are not obtained directly from a data subject, there can be an exception to this transparency obligation if the provision of the information would involve a disproportionate effort or the handling of the personal data is necessary for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract. If a data controller wishes to use the disproportionate effort exemption, the data controller must create a record of why it is a disproportionate effort.

4.4 When

The information should be provided at the time when the data controller first processes the data. Alternatively, where disclosure to a third party is envisaged within a reasonable period, the information should be provided when the data are first disclosed.

4.5 How

There is no particular form in which the information must be provided.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

Data subjects are entitled to exercise a right of access to their personal data against data controllers. The right must be exercised the writing. Often data controllers have a specified form which must be completed. Data controllers have the right to ask for such information as is reasonably necessary to enable them to locate the information.

5.1.2 Exceptions

There are a number of exceptions to the right, including:

- national security;
- prevention or detection of crime and the apprehension or prosecution of offenders or assessment and collection of tax;
- regulatory activities (eg enforcing regulation designed to prevent dishonesty, malpractice or improper conduct);
- journalism;
- employment or educational references given by a data controller (but not those received by a data controller);
- negotiations between the data controller and the data subject (if to disclose the information would be likely to prejudice the negotiations);
- management forecasting or planning information (if to disclose the information would be likely to prejudice the business); and
- information protected by legal professional privilege.

Additionally, if the information requested includes information about another identified individual, the data controller is not obliged to provide the information requested unless the other individual has consented to the disclosure of their information or it is reasonable in all the circumstances to disclose the information without that individual's consent.

5.1.3 Deadline

Data controllers are required to respond within 40 days of receiving a request. However the 40 day deadline is extended where a data controller is waiting for details from the requester to enable the data controller to find the requested information or is waiting for payment of the required charge.

5.1.4 Charges

In general the charge is £10 although in some circumstances it can be different (eg for credit rating reports the charge is £2 and for some medical records the charge can be £50).

5.2 Rectification

5.2.1 Right

If a court is satisfied on the application of a data subject that personal data are inaccurate then the court may order a data controller to rectify, block, erase or destroy those data.

Where a third party has received inaccurate data from a data controller, the court may also order the data controller to notify the third parties of the rectification, blocking, erasure or destruction of the data.

5.2.2 Exceptions

There are a number of exceptions to the right, including for the purposes of:

- national security;
- prevention or detection of crime and the apprehension or prosecution of offenders or assessment and collection of tax;
- journalism;
- public registers; and
- disclosures made by law or in connection with legal proceedings.

5.2.3 Deadline
The deadline for the rectification depends on the order of the court, as no time period is specified in the DPA.

5.2.4 Charges
There are no specific charges for rectification, but an individual would need to make an application to the court to enforce this right.

5.3 Erasure
Please see section 5.2.1 above. The right of erasure is in the same section of the DPA as the rectification right and follows the same procedure.

5.3.1 Right
See section 5.2.1 above.

5.3.2 Exceptions
See section 5.2.1 above.

5.3.3 Deadline
See section 5.2.1 above.

5.3.4 Charges
See section 5.2.1 above.

5.4 Blocking
Please see section 5.2.1 above. The blocking right is in the same section of the DPA as the rectification right and follows the same procedure.

5.4.1 Right
See section 5.2.1 above.

5.4.2 Exceptions
See section 5.2.1 above.

5..3 Deadline
See section 5.2.1 above.

5.4.4 Charges

See section 5.2.1 above.

5.5 Objection
5.5.1 Right
An individual is entitled, at any time by notice in writing to a data controller, to require the data controller at the end of such period as is reasonable in the circumstances to cease or not begin processing any personal data in respect of which he is the data subject. This must be on the basis that the processing is causing or is likely to cause substantial damage or substantial distress to him

or another person and such damage or distress would be unwarranted.

5.5.2 Exceptions

There are a number of exceptions to the right, including for the purposes of:

- national security;
- prevention or detection of crime and the apprehension or prosecution of offenders or assessment and collection of tax;
- journalism;
- public registers; and
- disclosures made by law or in connection with legal proceedings.

5.5.3 Deadline

The deadline for stopping the processing is such period as is reasonable in the circumstances. Upon receiving a notice from a data subject in the terms of section 5.5.1 above, a data controller must respond within 21 days stating that he has complied (or will comply) with the notice or explaining why it is an unjustified notice.

5.5.4 Charges

None.

5.6 Automated individual decisions

5.6.1 Right

An individual is entitled at any time by notice in writing to any data controller to require the data controller that no decision is taken by or on behalf of the data controller which significantly affects the individual and is based solely on processing by automatic means for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct.

5.6.2 Exceptions

This right does not apply where the decision is taken in the course of steps taken:

- in order to enter into a contract or perform a contract with the data subject or steps required by legislation; and
- the effect of the decision is either to grant a request of the data subject or steps have been taken to safeguard the legitimate interests of the data subject (eg by allowing him to make representations).

5.6.3 Deadline

Within 21 days of receiving a notice from the data subject the data controller must respond to the data subject specifying the steps he intends to take to comply with the notice.

5.6.4 Charges

None.

5.7 Other rights

None

5.7.1 Right
Not applicable.

5.7.2 Exceptions
Not applicable.

5.7.3 Deadline
Not applicable.

5.7.4 Charges
Not applicable.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who
Only data controllers are required to notify under the DPA.

6.1.2 What
Notification of data processing being carried out must be made to the ICO. This notification is made by the legal entity carrying out the processing. (There is no requirement to submit separate notifications for each database or each purpose. Also, there is no requirement for notification of data transfers).

6.1.3 Exceptions
There are exemptions for small businesses and/or businesses carrying out what are considered to be low risk or standard processing. These exemptions apply to data controllers who only process personal information for:

- staff administration (including payroll);
- advertising, marketing and public relations (in connection with your own business activity); and
- accounts and records.

Additionally, the following data controllers can be exempt from notification:

- Some not-for-profit organisations.
- Individuals processing personal information for personal, family or household affairs (including recreational purposes).
- Data controllers who only process personal information for the maintenance of a public register.
- Data controllers who do not process personal information on computer.

6.1.4 When
Notifications are made annually. Once notified a data controller should receive an annual renewal reminder from the ICO.

6.1.5 How
Notification is generally commenced by telephoning the ICO and partially completing a form over the phone. The form is then sent by the ICO to the

data controller to complete and submit with payment. Alternatively the form can be printed from the website, completed and submitted with payment to the ICO. At present there is no simple online notification process.

Details of the notification form can be found online at *www.ico.gov.uk*. The form will detail: the data controller; the types of data being handled; the sources of the data; the recipients of the data; the purposes of processing; and the countries to which data may be sent. In addition, the notification will include some details of security (which is not be made public on the register, see section 6.3.1 below). No further documents have to be submitted with a notification.

Notification is generally relatively quick as it is administrative and does not require any evaluation on the part of the ICO.

6.1.6 Notification fees

The fee for notification is £35 for most organisations, however, for large organisations (turnover of £25.9 million and 250 or more staff or public bodies with 250 or more staff) there is a £500 fee. The notification fee must be paid annually to the ICO and is used by the ICO to cover its data protection compliance work.

6.2 Authorisation requirements

Subject to approval of BCR applications (see section 8.2.2), there are no specific authorisation requirements under the DPA.

6.2.1 Who

Not applicable.

6.2.2 What

Not applicable.

6.2.3 Exceptions

Not applicable.

6.2.4 When

Not applicable.

6.2.5 How

Not applicable.

6.2.6 Authorisation fees

Not applicable.

6.3 Other registration requirements

There are no prior checking or other registration requirements.

6.3.1 Register

The ICO holds a register of data controllers. This is publically available through the ICO's website at *www.ico.gov.uk*. In 2011 the ICO plans to

make available DVDs/discs containing the register so that this is more easily accessible (this is because at present only a limited number of searches can be carried out through the ICO's website). At present it is free to consult the register on the website. It is not clear whether there will be a charge for the DVD.

The register contains the name and address of the data controller, the purposes for which personal data are processed and under each purpose the types of personal data, sources, recipients and countries to which the personal data are transferred.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

Under the DPA there is no official recognition of the role of a data protection officer (DPO). However, it is becoming increasingly common for UK businesses of a significant size or handling significant amounts of personal data to appoint a DPO.

7.2 Tasks and powers

As the role is not officially recognised under the DPA there is no specific set of rules or responsibilities or implications for appointing a DPO.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The eighth data protection principle in the DPA states that personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

8.2 Legal basis for international data transfers

Further interpretation of the eighth data protection principle under the DPA states that an adequate level of protection is one which is adequate in all the circumstances having particular regard to:

- the nature of the personal data;
- the country or territory of origin of the information;
- the country or territory of final destination of the information;
- the purposes for which and period during which the data are intended to be processed;
- the law in force in the country or territory in question;
- the international obligations of that country or territory;
- the relevant codes of conduct enforceable in that country or territory; and
- any security measures taken in respect of the data.

Additionally the DPA lists a number of cases where the eighth data protection principle does not apply and therefore personal data may be transferred outside the EEA, these are:

- the data subject has given his consent to the transfer;
- the transfer is necessary for the performance of a contract between the

data subject and the data controller or the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
- the transfer is necessary for the conclusion of a contract between the data controller and a third party which is entered into at the request of the data subject or in the interests of the data subject or for the performance of such contract;
- the transfer is necessary for reasons of substantial public interest;
- the transfer is necessary for the purpose of or in connection with any legal proceedings including prospective legal proceedings, is necessary for the purpose of obtaining legal advice or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the data subject;
- the transfer is of part of a public register;
- the transfer is made on terms which have been approved by the ICO (for example, the ICO has approved the European Commission's standard contractual clauses for data transfers); or
- the transfer has been authorised by the ICO. However, the ICO has a policy of not approving or authorising individual transfers, so in practice this exemption does not apply.

Finally, there is no public or private register or collection of information relating to international data transfers. The only way in which information relating to international data transfers is recorded is in the annual notifications (as mentioned above) or if the ICO issues an approval of binding corporate rules (BCRs). There is no requirement to obtain the ICO's prior approval of any international data transfers.

8.2.1 Data transfer agreements

The ICO has approved use of the European Commission's standard contractual clauses for transfers between data controllers and from data controllers to data processors.

Additionally, ICO guidance on the transfer of data outside the EEA emphasises that it is possible for data controllers to make their own decision on adequacy and one part of that may be having in place a contract. Therefore it is not necessary in the ICO's view to use the European Commission's standard contractual clauses to show adequacy.

A particular example where this may be useful is if there is sub-processing in place and the sub-processing does not strictly follow the sub-processing envisaged by the EU Model Clauses (eg where the data controller and data processer are both inside the EEA and the sub-processer is outside the EEA). In these circumstances the ICO guidance indicates that making some amendments to EU Model Clauses to fit the circumstances could show adequacy.

EU Model Clauses are however commonly used in the UK as it is clear that these will meet the adequacy requirements.

8.2.2 Binding corporate rules

Binding corporate rules have for some time been strongly promoted by the

ICO. The ICO follows the Article 29 Working Party papers and a number of UK organisations have already successfully applied for binding corporate rules approval.

The ICO recommends the completion of the application form in Article 29 Working Party WP 133 in order to apply to the ICO for BCR approval. Once received, the ICO would assess the application and, if approved, issue an authorisation, which is then published on the ICO website. The ICO participates in the mutual recognition procedure (by which 19 member states have agreed that if the lead authority approves the BCR application then the other member states should also approve).

8.2.3 Safe Harbour

The US Safe Harbour arrangement allowing transfers from the UK to the US is commonly used in the UK. Frequently these types of transfers are backed up by contractual clauses which require the US recipient of personal data to maintain Safe Harbour notification and to inform the UK data exporter of any change in the US data importer's Safe Harbour status.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Data processors are required to process information only on instructions from the data controller and a data controller is required to ensure that this is covered in the contract between the data controller and the data processor.

9.2 Security requirements

Under the DPA a data controller is required to ensure appropriate technical and organisational measures. This is further interpreted under the DPA by provisions which state that the data controller must: (i) have regard to the state of technological development and the cost of implementing any measures; and (ii) ensure the level of security is appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data. The ICO has issued some guidance on interpreting the security requirements (for example on the value in staff vetting, training and monitoring). There is limited guidance on technological matters. However the ICO has issued guidance that laptops and removable media containing personal data should be encrypted and that failure to ensure encryption is likely to result in enforcement action if the relevant laptop or removable media (containing unencrypted personal data) is then lost.

9.3 Data security breach notification obligation

Under the DPA there is no obligation to make a data security breach notification. However there is good practice guidance from the ICO that in some circumstances notification should take place. It is this good practice guidance that is described below.

There are specific requirements for communications providers to make notifications of breaches to the ICO (as provided in the e-Privacy Directive 2009 and implemented in the UK in 2011). As these requirements are specific

to communications providers only they are not discussed below.

9.3.1 Who
The data controller is required to notify under the ICO guidance.

9.3.2 What
The ICO has issued guidance on the information it recommends providing to the ICO in relation to a security breach and has prepared a short form that can be used for notification. The information to be provided includes circumstances of the breach, individuals affected and remedial steps taken.

9.3.3 To whom
The guidance recommends notifying the ICO. Additionally, the guidance states that it may be necessary to notify the individuals affected in some cases.

9.3.4 When
There is no particular time in which notification must be made. The ICO guidance recommends notification if personal data affecting 1,000 or more individuals are lost, or if sensitive data are lost, then as few as 10 lost records could trigger a notification.

9.3.5 How
There is no required format for notification, although as mentioned above the ICO has prepared a standard form listing the relevant topics to be covered in any notification (see *www.ico.gov.uk*).

9.3.6 Sanctions for non-compliance
As there is no legal requirement for notification generally, there is no sanction for failure to notify. However, the ICO states that it will be more lenient on organisations that voluntarily notify compared to those who make no notification and wait for the ICO to discover the breach.

9.4 Data protection impact assessments and audits
There is no legal requirement to carry out privacy impact assessments, although these are recommended by the ICO in public sector data projects and for intrusive actions such as monitoring. The ICO has issued comprehensive guidance on carrying out privacy impact assessments, which is primarily aimed at government data handling projects. It is a requirement of UK central government projects that a privacy impact assessment be completed (although this does not need to be comprehensive).

There is a legal requirement to submit to audits which is applicable only to central government bodies, not to the wider public sector nor to the private sector. The ICO is campaigning to get the right to audit any private or public sector body.

9.4.1 Who
The ICO can audit central government bodies.

9.4.2 What
The audit is of compliance with the DPA.

9.4.3 When
In general the ICO tries to agree audits (ie to arrange a consensual audit) even though it has the right to compulsorily audit central government bodies.

9.4.4 How
The ICO will agree the scope of the audit in writing, review paperwork provided by the data controller and visit the relevant data controller to carry out interviews and check practices on the ground. There is then a written audit report, a summary of which is published by the ICO.

Since September 2010, the ICO has carried out 37 consensual audits within both the public and private sectors. Summary results of the audit findings are published on the ICO's website, unless the audited body refuses, in which case a note is published on the ICO's website to the effect that an audit was carried out but there was no consent to publish a summary of the findings.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action
Enforcement action is taken by the ICO rather than any other bodies. It is possible for some rights (eg the right to compensation) to be enforced through the courts, but this is not a frequent occurrence due to the costs of enforcing through court action. Most complainants prefer to inform the ICO and ask the ICO to investigate.

The majority of complaints are dealt with through consultation and agreement between the parties. That said, the ICO has developed a practice, especially in cases of data losses, of using Chief Executive Officer undertakings. These are written undertakings signed by a CEO of a data controller in which the CEO recites the failings of his/her company and confirms in writing the steps that will be taken to prevent recurrence. The undertaking is then published on the ICO website. This is not a process set out in the DPA and has arisen in practice over recent years as it is considered to be effective and low cost (to the ICO).

More formal enforcement would include enforcement notices, which are issued relatively rarely. These are orders requiring a data controller to remedy certain processing activities. For example, in 2010 the ICO issued just three enforcement notices, each concerned with automated or unsolicited marketing phone calls.

Since April 2011 the ICO has had the power to fine up to £500,000 for serious breaches of the DPA and has issued, as at the date of writing, only six fines. Most of these fines have been between £50-100,000. There is a reduction of 20 per cent for early payment. The fines have been issued due to data losses/breaches and usually due to the loss or theft of unencrypted laptops/media.

10.2 Sanctions
Criminal sanctions are available for failure to notify with the ICO or failure to

have an up to date notification. There are relatively few criminal prosecutions for these offences (approximately 10 per year).

Criminal sanctions are also available for obtaining personal data illegally (eg pre-texting or blagging, which occurs when a person impersonates another usually to obtain personal data over the phone). It is claimed that many private investigators use this method of obtaining information. In particular the ICO has highlighted the use by the newspaper industry of private investigators using blagging to obtain information for newspaper reports.) The ICO has carried out prosecutions for these offences, again usually only a couple of prosecutions in any year.

10.3 Examples of recent enforcement of data protection rules

As mentioned above, the most active area for ICO enforcement is security breaches. In these cases the ICO tend to use CEO undertakings as described above, and in some circumstances fines. Use of criminal sanctions is most unusual.

10.4 Judicial remedies

A number of rights (eg subject access) can be enforced through the courts. Individuals also have the right to claim compensation (see below). That said, it is most unusual to have cases purely on data protection issues. Often cases relate to confidential information and data protection issues are a subsidiary part of the claim. Alternatively data protection issues may be raised in employment claims. No official figures as to the number of claims are publicly available.

The ICO does not normally initiate judicial proceedings on data protection matters (it would be for data subjects to bring judicial proceedings).

10.5 Class actions

Class actions in general are not common in UK law, and at the date of writing we are not aware of any data protection class actions.

10.6 Liability

Data controllers can be held liable to pay compensation for damage and distress caused to a data subject by breach of the DPA. There is a defence against such claims if the data controller has taken reasonable care. Claims are not commonly reported, but may occur and be settled informally. Reported cases involving claims for damage and distress have resulted in very small payments, but this is often because a larger damage claim has been awarded on the same facts for breach of confidence (for example data protection compensation of £50, but breach of confidence damages for many thousands of pounds). Consequently, the case law is not conclusive on the value of data protection compensation.

Note also that it is necessary for a claimant to show both damage and distress, as it is not possible under the DPA to claim purely for distress. This aspect of the DPA is under review by the European Commission as not meeting the requirements of the Directive.

United States of America

Foley & Lardner LLP
Andrew Serwin, Daniel Muto & Megan O'Sullivan

1. LEGISLATION

Unlike the European Union, the US does not have a singular law to provide comprehensive treatment of privacy or data security issues. Instead, the US approach has instead been to pass specific and narrowly applicable legislation (both state and federal) aimed at preventing specific privacy harms or protecting particular types of sensitive data.

1.1 Name/title of the law

The main relevant laws are:

- Federal Trade Commission Act (FTC Act, FTCA or Section 5);
- Health Insurance Portability and Accountability Act (HIPAA);
- Gramm-Leach-Bliley Act (GLB).

1.2 Pending legislation

FTCA

The FTC's interest in consumer protection is underscored by a December 2010 report entitled *'Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers'* pursuant to which the FTC identified a four-part framework to govern commercial use of consumer data. Specifically, the report encouraged companies to: (i) adopt a 'privacy by design' approach by building privacy protections into their everyday business practices; (ii) provide a more streamlined way for consumers to exercise choice with respect to the commercial use of their data; (iii) make their data practices more transparent; and (iv) undertake a broad effort to educate consumers about commercial data practices and the choices available to them. The report also encouraged interested parties to raise and comment upon related privacy issues, but noted that in the meantime the FTC would vigorously continue its enforcement efforts in the privacy arena under its Section 5 authority. A similar focus on improving the privacy of consumer data can be found in recent initiatives by both the US Department of Commerce (see Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, December 2010) and the White House (which has launched the National Strategy for Trusted Identities in Cyberspace initiative to work collaboratively with the private sector,

advocacy groups, public sector agencies, and other organisations to improve the privacy, security, and convenience of sensitive online transactions).

These privacy initiatives appear to have resonated with US legislators, and as a result privacy and data security have become hot topics for Republicans and Democrats alike. Indeed, there are currently several laws pending in Congress that aim to address a variety of privacy and data protection concerns. In the House of Representatives, for example, proposals range in scope from implementing a national security breach notification law (eg, the SAFE Data Act, H.R. 2577), to extending and enhancing existing online privacy protections for children and teens (eg, the Do Not Track Kids Act of 2011, H.R. 1895), to requiring reasonable security policies and procedures to protect computerised data containing personal information (eg the Data Accountability and Trust Act of 2011, H.R. 1841). The legislative focus on privacy has also reached the Senate, where in April of 2011 Senators John Kerry and John McCain introduced the Commercial Privacy Bill of Rights Act of 2011 (S. 799), the first comprehensive privacy bill introduced to the Senate in over a decade.

If enacted, many of the proposed laws would drastically alter the privacy landscape in the United States; however, they have generally failed to garner the requisite support in Congress and do not appear likely to become law.

HIPAA

There is no known pending legislation under HIPAA.

However, some states are expanding citizens' right to privacy even broader than HIPAA or the Health Information Technology for Economic and Clinical Health (HITECH) Act , a recent amendment to HIPAA that expanded its coverage, requires. For instance, Texas recently passed a law, effective 1 September 2012, which is significantly more stringent than HIPAA or HITECH. Specifically, Texas House Bill 300 increases the employee training covered entities must conduct regarding 'the state and federal law concerning protected health information.' While HIPAA requires employee training, it does not set a timeline; H.B. 300 mandates that new employees must be trained within 60 days of hiring. Similarly, H.B. 300 requires that employees receive training every two years; HIPAA has no such requirement.

Accordingly, specific states' laws regarding the privacy of protected health information may be more stringent than the following discussion of HIPAA and HITECH suggests.

GLB

There is no known pending legislation under GLB.

1.3 Scope of the law

FTCA

The US relies heavily on the broad consumer protection authority granted to the Federal Trade Commission (FTC or the Commission) by FTCA to address data protection issues that affect consumers. Specifically, the FTC's authority to prevent 'deceptive' and 'unfair' acts or practices under section 5 of the FTCA (Section 5) has allowed the FTC to play a central role in privacy

enforcement in the United States. While the FTC is also responsible for the enforcement of a number of other federal laws - including the Fair Credit Reporting Act (FCRA), GLB, and the Children's Online Privacy Protection Act (COPPA) - which impose specific data protection requirements on covered entities who collect and process personal information, the FTC's deception and unfairness authority under Section 5 serves as the FTC's principal basis for privacy and data security enforcement.

HIPAA

HIPAA governs the use and disclosure of protected health information (PHI) through the imposition of privacy, security and reporting requirements, as well as marketing restrictions.

HIPAA arose not from concerns over privacy, but as part of the debate over national health care. While the law has significant privacy implications, it is not a law directed exclusively at privacy.

The HIPAA portion of the chapter will discuss the HIPAA's privacy requirements (the HIPAA Privacy Rule) and HIPAA's rules regarding the security of electronic protected health information (the HIPAA Security Rule).

GLB

In order to ensure that financial institutions protect the privacy of their customers, GLB imposes privacy and security regulations on certain financial institutions if they collect 'non-public personal information.'

1.3.1 The main players

FTCA

The FTC is *'empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce.'* To this end, the FTC may prevent persons, partnerships or corporations from using unfair or deceptive acts or practices in or affecting commerce. Thus, the main players under Section 5 are (i) the FTC and (ii) entities whose business practices affect commerce and consumers.

HIPAA

HIPAA's provisions apply to 'covered entities,' defined as: (i) a health plan; a (ii) a health care clearinghouse; or (iii) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

HIPAA's rules also apply to covered entities' business associates. 'Business associate' is defined as a person who: (i) 'performs, or assists in the performance of': a function or activity involving the use or disclosure of individually identifiable health information; or (ii) provides services involving the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. Each business associate is required to enter into a written contract. A covered entity may permit a business associate to create,

receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

GLB

GLB was enacted to ensure that financial institutions who collect 'non-public personal information' meet their obligations to customers to protect customer privacy and to implement safeguards to protect customers' information. 'Financial institution' is defined as any institution the business of which is engaging in financial or persons subject to the Commodity Futures Trading Commission (CFTC). The term 'financial institution' does not include any person or entity with respect to any financial activity that is subject to the jurisdiction of the CFTC under the Commodity Exchange Act; farm credit institutions, or any other secondary market institutions.

1.3.2 Types of data

FTCA

The FTC's Section 5 authority is defined without reference to particular types of data. However, recent enforcement actions suggest that the FTC believes it has the authority to regulate 'personal information' or 'covered information,' which the FTC has defined on at least one occasion as: *'Information [an entity] collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above.'*

HIPAA

PHI is 'individually identifiable health information' that is not contained in education or employment records and includes any information that is written, oral, or transmitted by or stored in electronic media. Individually identifiable information is defined as information that is a subset of health information, including demographic information collected from an individual that: (i) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (ii) relates to the past, present, or future mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of the health care to an individual; and (iii) identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

GLB

GLB only applies to 'non-public personal information.' Non-public personal information (NPI) means personally identifiable financial information that: (i) is provided by a consumer to a financial institution; (ii) results from any

transaction with the consumer or any service performed by the consumer; or (iii) is otherwise obtained by the financial institution.

NPI does not include: (i) publicly available information generally; or (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

NPI includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers. NPI does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

1.3.3 Types of acts/operations

FTCA

Section 5 is a consumer-facing data collection law that empowers and directs the FTC to prevent 'unfair methods of competition […] and unfair or deceptive acts or practices in commerce.' This language has been interpreted as affording the FTC with two separate avenues for enforcement, which are known respectively as its 'unfairness' and 'deception' authority. These terms are not defined in the FTCA itself, but in a policy statement to Congress the FTC identified several key elements that it considered when assessing whether a business practice was deceptive (the 'Deception Statement'). The Deception Statement suggests that an act or practice is deceptive in the eyes of the FTC if: (i) there is a representation, omission, or practice; (ii) that is likely to mislead consumers acting reasonably under the circumstances; and (iii) the representation, omission, or practice is material. Importantly the FTC has since noted that an act or practice does not necessarily need to result in actual deception to satisfy the second element of deception noted above. With respect to the materiality element, the FTC has indicated that a representation, omission, or practice is material if it was important to the consumer, which means that information is deemed material if it *'is likely to affect a consumer's choice of or conduct regarding a product.'*

In addition to its deception authority, the FTC is also authorised to prevent unfair practices in or affecting commerce. This unfairness authority has been clarified over time. Specifically, the FTC issued what has since become known as the 'Unfairness Statement,' pursuant to which the FTC stated its own understanding regarding the parameters of its unfairness authority. The Unfairness Statement focused heavily on whether or not a practice would lead to consumer injury in order to determine whether the practice fell within the scope of the FTC's unfairness authority. To this end, the FTC identified three factors that it would use to determine if there was sufficient consumer injury: (i) there must be substantial consumer injury; (ii) that is not outweighed by any offsetting consumer or competitive benefits that the sales practice also produces; and (iii) the injury must be one which consumers could not have reasonably avoided. The consumer injury focus of the FTC's unfairness

authority was eventually codified by Congress via an amendment to Section 5 that mirrors the factors identified in the Unfairness Statement.

HIPAA

A major purpose of HIPAA is to define and limit the circumstances under which an individual's PHI may be used or disclosed by covered entities. A covered entity may not use or disclose PHI, except either: (i) as HIPAA's Privacy Rule permits or requires; or (ii) as the individual who is the subject of the information (or the individual's personal representative) authorises in writing.

A covered entity is permitted to disclose PHI: (i) to the individual (unless required for access or accounting of disclosures); (ii) for treatment, payment, and health care operations; (iii) uses and disclosures with the opportunity to agree or object; (iv) when disclosure is incident to an otherwise permitted use and disclosure; (v) for the public interest and benefit; and (vi) with a limited data set for the purposes of research, public health or health care operations.

A covered entity is required to disclose PHI only: (i) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and (ii) to the Department of Health & Human Services (HHS) when it is undertaking a compliance investigation or review or enforcement action.

GLB

Financial institutions are required to protect customer privacy and to implement administrative, technical and physical safeguards (see section 9 below).

One of GLB's main requirements is that notice must be given to consumers regarding a variety of issues (see section 4 below).

GLB also precludes the practice of obtaining financial information under false pretences. The statute expressly prohibits a person from obtaining, attempting to obtain, or causing someone to disclose to any person, customer information of a financial institution relating to another by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution, making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution, or providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.

1.3.4 Exceptions

FTCA

With limited exceptions, Section 5 grants the FTC jurisdiction over nearly every economic sector. Certain entities, such as depository institutions and common carriers, as well as the business of insurance, are wholly or partly exempt from the FTC's jurisdiction.

HIPAA

The definition of PHI specifically excludes information stored in employment records.

GLB

GLB does not preclude the disclosure of NPI by a financial institution in the following eight circumstances: (i) to a third party to perform services for or functions on behalf of the financial institution, including marketing; (ii) if the disclosure is necessary to effect a transaction requested by the consumer or maintain the consumer's service, or with another entity as part of the financial institution's private label credit card or other extension of credit; (iii) if the disclosure is related to a proposed or actual securitisation, secondary market sale, or similar transaction related to a transaction to the customer; (iv) to the extent specifically allowed or required under other provisions of law, in accordance with the Right to Privacy Act of 1978, to law enforcement agencies, self-regulatory organisations, or for a matter involving public safety; (v) to a consumer reporting agency in accordance with the FCRA, or if required by Federal, state, or local laws; (vi) disclosure can be made to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service, product, or the transaction, to protect against or prevent actual or potential fraud, unauthorised transactions, claims, or other liability, for required institutional risk control, or for resolving customer disputes or inquiries; (vii) disclosure can also be made to persons holding a legal or beneficial interest relating to the consumer or to persons acting in a fiduciary or representative capacity on behalf of the consumer; and (viii) disclosure can be made with the consent, or at the direction, of the consumer, to provide information to insurance rate advisory organisations, guarantee funds or agencies, of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors, or in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of NPI concerns solely consumers of such business or unit.

Pursuant to a judgment by the Appellate Court, attorneys are not 'financial institutions' and are therefore not subject to GLB.

1.3.5 Geographical scope of application

FTCA

The FTC's enforcement authority is not subject to geographical restrictions, provided that the allegedly unfair or deceptive business practice must be in or have a substantial effect on US commerce.

HIPAA

Generally, a standard, requirement or implementation specification that is contrary to a provision of state law pre-empts the provision of state law.

GLB

GLB pre-empts state law to the extent that state law provides lesser protection than does GLB. However, if the state law provides greater protection, the law is not pre-empted.

1.4 Particularities

FTCA

None.

HIPAA

None.

GLB

As part of the rulemaking for GLB, the FTC issued the Financial Privacy Rule, which requires financial institutions to have measures in place to keep customer information secure. The Office of Comptroller of the Currency (OCC), Federal Reserve System, Federal Deposit Insurance Corporation, the Office of Thrift Supervision, National Credit Union Administration, FTC, Commodity Futures Trading Commission and the Security and Exchange Commission have jointly issued rules under GLB, including the often discussed model privacy notice. The model privacy notice is intended to make it easier for consumers to understand how financial institutions collect and share information about consumers. At this time many financial institutions are taking a 'wait and see' approach to the model notice, as it is suggested and provides a safe harbour, but it is not mandated at this time.

2. DATA PROTECTION AUTHORITY

FTCA

Name: Federal Trade Commission
Address: 600 Pennsylvania Avenue, NW, Washington D.C., 20580, USA
Telephone: 1-877-FTC-HELP (1-877-382-4357)
Fax: Not Available
E-mail: Not Available
Website: *www.ftc.gov*

HIPAA

Name: Office for Civil Rights – US Department of Health & Human Services (HHS)
Address: 200 Independence Avenue, S.W., Room 509F HHH Bldg., Washington, D.C. 20201, US
Telephone: (800) 368-1019
Fax: (617) 565-3809 (Boston Office)
E-mail: OCRMail@hhs.gov
Website: *www.hhs.gov/ocr/*

GLB

As FTC above

2.1 Role and tasks

FTCA

The FTC is specifically charged with enforcing a number of federal statutes, but the main source of its privacy jurisdiction is based upon 'unlawful' practices

under the FTCA. A practice is 'unlawful' to the extent it violates Section 5 or Section 12 of the FTCA. Section 12 prohibits false advertisements, whereas Section 5 prohibits deceptive and unfair acts or practices and specifically empowers the FTC to 'prevent persons, partnerships, or corporations […] from using unfair or deceptive acts or practices in commerce.'

HIPAA

HHS is the relevant authority to enforce HIPAA.

GLB

There are a number of agencies that have enforcement authority, depending upon the type of financial institution. The FTC, state insurance authorities, as well as the Federal functional regulators, including the Board of Governors of the Federal Reserve System, the OCC, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, the National Credit Union Administration Board, and the Securities and Exchange Commission, all have enforcement power.

2.2 Powers

FTCA

The FTC essentially has two options regarding how to move forward once it has determined that an unfair or deceptive trade practice is occurring: (i) bring suit in federal court to obtain appropriate equitable relief - including restitution to either domestic or foreign victims, discouragement, and either a temporary restraining order or a preliminary injunction pending the initiation of administrative action; or (ii) proceed exclusively in federal district court by filing a complaint seeking a permanent injunction and ancillary relief, including temporary or preliminary injunctive relief. In addition to injunctive relief, the FTC can seek asset freezes, the appointment of a receiver, and discouragement or restitution of ill-gotten gains.

HIPAA

HHS can bring enforcement actions for violations of HIPAA as well as issue civil monetary penalties.

GLB

Enforcement powers under GLB (similar to those under the FTCA) are explicitly shared between the Bureau of Consumer Financial Protection, Federal functional regulators, State insurance authorities, and the FTC.

2.3 Priorities

FTCA

Today the FTC is primarily focused on preventing business practices that cause harm to consumers. However, the FTC's focus has shifted dramatically over time, as it was originally created in 1914 in order to protect competition between businesses. The FTC of 2011 brands itself as the 'nation's consumer protection agency' and has a self-professed agenda 'to prevent fraud,

deception, and unfair business practices in the marketplace.'

Recently, the FTC announced a privacy agenda that provides some insight into what it considers to be improper practices that could lead to a Section 5 enforcement action. Additional guidance regarding the FTC's privacy agenda can be gathered from the pattern of recent Section 5 enforcement actions brought by the FTC. Taken together, these factors indicate that the FTC's current agenda includes: (i) stepping up the enforcement of spam laws (eg, taking steps to limit chain letters and pyramid schemes); (ii) increasing assistance to victims of identity theft (eg identifying reported patterns in conduct and creating a unified fraud affidavit for victims); (iii) enforcing the terms of companies' privacy promises to consumers (eg, promises made in privacy or data protection policies); (iv) focusing especially on cases involving sensitive information, transfers of information in bankruptcy and practices that violate the US-EU Safe Harbour program; and (v) increasing enforcement of GLB and COPPA.

HIPAA

In 2010, the top five issues investigated by HHS in relation to HIPAA violations were, in order: (i) impermissible uses and disclosures of PHI; (ii) safeguards for PHI; (iii) access; (iv) only disclosing the minimum PHI necessary; and (v) notice. No such statistics have been announced for 2011.

GLB

None.

3. LEGAL BASIS FOR DATA PROCESSING

FTCA

The FTC's Section 5 authority is defined without reference to the types of data processing activities that fall within its scope. However, recent enforcement actions suggest that the FTC has interpreted Section 5 as broadly applying to any data processing activities that constitute unfair or deceptive acts or practices in the marketplace. Examples of such activities include: (i) collecting more personal information from consumers than is indicated in a website's privacy policy; (ii) disclosing personal information to third parties in a manner that is inconsistent with representations made in a privacy policy; and (iii) failing to take steps to protect personal information which are proportional to, or in accordance with, representations in a privacy policy.

HIPAA

HIPAA's regulations cover the use and disclosure of PHI.

GLB

GLB covers the disclosure of NPI.

3.1 Consent

3.1.1 Definition

FTCA

Section 5 does not explicitly impose consent requirements for data

processing activities. However, various FTC enforcement actions suggest that companies may be required to obtain 'opt-in' or 'opt-out' consent under certain circumstances. To this end, the FTC has noted that 'opt-in' consent requires a company to obtain 'the express affirmative consent of the consumers to whom such personal information relates', whereas 'opt-out' consent allows a company to infer consent from a consumer's behaviour.

The FTC has generally required 'opt-in' consent only where a company desires to use personal information in a manner that is inconsistent with the company's stated privacy practices at the time the personal information was collected from a consumer. In a settlement agreement with Gateway Learning Corporation, for example, the FTC explicitly prohibited Gateway from disclosing 'to any third party any personal information collected on [Gateway's website] prior to the date Gateway posted its revised privacy policy permitting third party sharing' unless the company first obtained 'opt-in' consent from its consumers to do so. The FTC appears most likely to require 'opt-in' consent where it believes a company has made material changes to its privacy practices in a way that is deceptive or misleading to customers.

HIPAA

A covered entity 'may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.' However, consent is not sufficient 'to permit a use or disclosure of protected health information when an authorisation is required or when another condition must be met for such use or disclosure to be permissible under this subpart.'

GLB

A financial institution may disclose NPI at the consent of the consumer, provided that the consumer has not revoked the consent or direction.

3.1.2 Form

FTCA

'Opt-out' consent may be implied from a consumer's behaviour. For example, the terms of use on most websites state that continued use of the website implies that a user consents to the practices outlined in the website's terms of use. This allows the company to infer a user's consent from his or her decision to use the website.

By contrast, 'opt-in' consent requires a company to obtain a consumer's express consent to the practice in question. Thus, a consumer is generally required to take an affirmative action (eg, signing a consent form or clicking 'I agree' after reading a given disclosure) before a company is deemed to have obtained that consumer's 'opt-in' consent.

HIPAA

The covered entity has discretion as to how to obtain consent. HIPAA rules in effect prior to the August 2002 revisions regulated a covered entity's obtaining of consent, but the current rules do not.

GLB
None.

3.1.3 In an employment relationship

FTCA
The FTC is principally a consumer protection agency, and generally does not regulate data processing in an employment relationship.

HIPAA
HIPAA is generally not applicable to employers.

GLB
GLB is not applicable to employers.

3.2 Other legal grounds for data processing

FTCA
Not applicable.

HIPAA
In order for a covered entity to use or disclose PHI, that covered entity generally must 'obtain or receive a valid authorisation for its use or disclosure of protected health information, [and] such use or disclosure must be consistent with such authorisation.'

GLB
GLB does not preclude the disclosure of NPI by a financial institution in the eight circumstances described section 1.3.4.

3.3 Direct marketing and cookies

FTCA
While direct marketing and cookies are not directly covered or defined in Section 5, the FTC has issued specific guidance regarding how disclosures should be made on the internet, particularly in the context of internet advertising. To this end, the FTC specifically noted that its Section 5 authority encompasses internet advertising, marketing and sales, and that disclosures regarding such activities must be 'clear and conspicuous' so that customers are easily able to understand them. It recommends reviewing such disclosures from the perspective of a reasonable consumer and determining how the disclosure is perceived in the context of the advertisement. Factors that the FTC will consider in deciding if a disclosure meets the requisite standard include: the disclosure's proximity to the online advertisement; the prominence of the disclosure; and whether the language of the disclosure is understandable to the intended audience.

Additionally, the FTC recently issued guidance directly related to online behavioural advertising (OBA), which is entitled *Online Behavioural Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles*. This guidance defined the practice of OBA and identified the following five

key principles that should be followed by those who participate in OBA: (i) transparency and consumer control; (ii) reasonable security and limited retention for consumer data; (iii) affirmative express consent for material changes to existing privacy promises; (iv) affirmative express consent to (or prohibition against) using sensitive data for OBA purposes; and (v) using tracking data for purposes other than OBA.

It is important to note that the guidance's transparency principle would require companies to provide a clear, concise, consumer-friendly and prominent statement that: (i) data regarding consumers' online activities are being collected for OBA purposes; and (ii) consumers can choose whether to have their information collected for these purposes. The FTC did not simply prohibit OBA as it is seeking to balance support for innovation with the need to protect against harm to consumers' privacy.

The FTC has brought several enforcement actions under Section 5 that relate to direct marketing and the use of tracking technologies. The basis for such enforcement actions has typically been that it is a deceptive business practice for a company not to adequately disclose either the extent to which it collects personal information, or the extent to which it shares this information with third parties. However, the FTC has also indicated that it may enforce similar issues under its unfairness authority, even where a company has not made an affirmative misrepresentation to consumers.

HIPAA

The HIPAA Privacy Rule requires an individual's written authorisation before use or disclosure of that individual's PHI can be made for marketing purposes. The limited exceptions to this rule are if the communication is in the form of: (i) a face-to-face communication made by a covered entity to an individual; or (ii) a promotional gift of nominal value provided by the covered entity.

GLB

A financial institution may provide NPI to a non-affiliated third party to perform services for or function on behalf of the financial institution, 'including marketing of the financial institution's own products or services or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 504, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information.' However, a financial institution may not share an 'account number information for marketing purposes.' Specifically, 'a financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.'

3.4 Data quality requirements

FTCA

Not applicable.

HIPAA

When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

GLB

Not applicable.

3.5 Outsourcing

FTCA

Outsourcing is not specifically referenced in Section 5 and is not core to the FTC's enforcement authority. However, certain FTC enforcement actions address risk assessments of third party vendors to whom data processing responsibilities are outsourced, and therefore outsourcing may become relevant in the context of FTC settlement agreements. This is particularly true if the subject of the settlement agreement is also required to comply with other federal laws that require covered entities to take precautions with respect to outsourced data processing vendors or service providers (eg, GLB).

HIPAA

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

GLB

Not applicable.

3.6 Email, internet and video monitoring

3.6.1 General rules

The principal federal law in the US that regulates these issues is the Electronic Communications Privacy Act of 1986, but several states have also passed legislation that addresses monitoring of electronic communications. These issues are not directly addressed by the FTCA, HIPAA or GLB.

3.6.2 Employment relationship

Not applicable under the FTCA, HIPAA, or GLB.

4. INFORMATION OBLIGATIONS

FTCA

Section 5 does not impose information obligations vis-à-vis consumers as US law does not regulate privacy under this framework.

However, several FTC enforcement actions suggest that certain entities may be required to obtain consumer authorisation (ie 'opt-in' consent) prior to taking actions that are inconsistent with privacy promises that were in effect at the time personal data were collected from a consumer.

HIPAA
Not applicable.

GLB
GLB requires that notice be given to consumers regarding a variety of issues.

4.1 Who

FTCA
Not applicable.

HIPAA
Covered entities must give patients notice. A patient may ask for a copy at any time. The covered entity cannot use or disclose PHI in a way that is not consistent with this notice.

GLB
GLB requires that notice be given by covered entities to consumers regarding a variety of issues.

4.2 What

FTCA
Data processing entities may be required to obtain consumer authorisation prior to handling or collecting personal data in a manner that represents a change from the entity's stated privacy practices in effect at the time the personal data were collected from a consumer. For example, authorisation may be required before sharing with third parties any personal information collected on or through a website when, at the time the personal data were collected, the website's privacy policy did not adequately disclose to users: (i) that the website collects personal information which might be shared with one or more third parties; (ii) the identity or specific categories of such third parties; and (iii) the purpose(s) for sharing such information with third parties. The FTC is also authorised to require the deletion of personal information that was collected or shared in a manner inconsistent with stated privacy practices.

HIPAA
The privacy notice must describe: the ways that the privacy rule allows the covered entity to use and disclose PHI. It must also explain that the entity will get the individual's permission, or authorisation, before using his health records for any other reason; the covered entity's duties to protect health information privacy; the privacy rights, including the right to complain to HHS and to the covered entity if the individual believes his privacy rights have been violated; how to contact the entity for more information and to make a complaint.

GLB

The initial notice of a financial institution must describe the disclosure and information protection policies. Additionally, in order for a financial institution to disclose NPI to a third party, the financial institution must first issue the consumer with the notice regarding the financial institution's disclosure and information protection policies, but additionally must: (i) clearly and conspicuously disclose to the consumer that such information may be disclosed to a third party; (ii) give the consumer an opportunity before disclosure to opt out; and (iii) give the consumer an explanation of how the consumer can exercise the non-disclosure option.

4.3 Exceptions

FTCAEntities are not required to obtain authorisation to process personal information in accordance with their clearly and concisely stated privacy practices in effect at the time that such information is collected from the consumer. Processing personal information under these circumstances does not constitute an unfair or deceptive business practice, and therefore falls outside of the FTC's Section 5 authority.

HIPAA

There are no exceptions to this notification rule except in emergencies, described below.

GLB

The notice requirement does not prevent a financial institution from providing NPI in the eight circumstances discussed above in section 1.3.4.

4.4 When

FTCA

The focus of the FTC's analysis has typically been whether adequate disclosures regarding a company's data sharing practices were available to the consumer at the time personal information was collected from that consumer. Authorisation is required if a company intends to share personal information that was collected under a previous version of a privacy policy (ie, one that did not make adequate disclosures regarding the sharing of personal information with third parties), even if the privacy policy was subsequently amended to properly disclose the company's information sharing practices. The FTC has formulated the authorisation requirement as follows: *'In connection with the posting of any privacy policy that contains a material change from the previous version of the policy, [an entity] shall not apply such changes to information collected from or about consumers before the date of the posting, unless [it] obtains the express affirmative ('opt-in') consent of the consumers to whom such personal information relates.'*

HIPAA

Generally, this notice should be given to the patient on the first visit to a provider or in the mail from the patients' health insurance. HHS's guidance

provides that: *'Most covered health care providers must give notice to their patients at the patient's first service encounter (usually at your first appointment). In emergency treatment situations, the provider must give the patient the notice as soon as possible after the emergency. It must also post the notice in a clear and easy to find location where patients are able to read it. A health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan can give the notice to the 'named insured,' that is, the subscriber for coverage. It does not also have to give separate notices to any covered spouses and dependents. A covered entity must give a copy of the notice to anyone who asks for one. If a covered entity has a web site for customers, it must post its notice in an obvious spot there.'*

GLB

The financial institution must provide notice when a customer relationship is established with a consumer, and not less than annually thereafter during the relationship.

4.5 How

FTCA

Section 5 does not explicitly state the form that consumer authorisation must take. Several enforcement actions have required companies to maintain records of all 'opt-in' consent obtained from consumers for a certain period of time, but such actions have not specified a required form for those records.

HIPAA

A patient may ask for a copy at any time.

GLB

The notification must provide clear and conspicuous disclosure to the consumer in writing, electronic, or other form permitted by the regulations of the financial institution's policies and practices with respect to: (i) disclosing NPI to affiliates and non-affiliated parties, including the categories of information that may be disclosed; (ii) disclosing NPI of persons who have ceased to be customers of the financial institution; and (iii) protecting the NPI of consumers.

5. RIGHTS OF INDIVIDUALS

FTCA

Section 5 does not grant to consumers individual privacy rights, but rather authorises the FTC to take action on behalf of those consumers.

HIPAA

An individual may request an accounting of disclosures (ie, a listing providing information about when a covered entity discloses the individuals' information to others) from covered entities.

GLB
Not applicable.

5.1 Access

5.1.1 Right

FTCA
Not applicable.

HIPAA
Except as otherwise provided, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set.

GLB
Not applicable.

5.1.2 Exceptions

FTCA
Not applicable.

HIPAA
The access above is subject to exceptions for: psychotherapy notes; information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and PHI maintained by a covered entity that is: subject to the Clinical Laboratory Improvements Amendments of 1988, to the extent the provision of access to the individual would be prohibited by law, or exempt from the Clinical Laboratory Improvements Amendments of 1988.

A covered entity may deny an individual access without providing the individual an opportunity for review, in a number of circumstances. First, if the PHI is excepted from the right of access. Second, a covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardise the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate. Third, an individual's access to PHI created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research. Fourth, an individual's access to PHI that is contained in records that are subject to the Privacy Act may be denied, if the denial of access under the Privacy Act would meet the requirements of that law. Finally, an individual's access may be denied if the PHI was obtained from someone other than a health

care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed in certain circumstances. This includes if: a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; the PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

GLB
Not applicable.

5.1.3 Deadline
Not applicable.

5.1.4 Charges
Not applicable.

5.2 Rectification
5.2.1 Right
FTCA
Not applicable.

HIPAA
An individual has the right to have a covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

GLB
Not applicable.

5.2.2 Exceptions
FTCA
Not applicable.

HIPAA
A covered entity may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request: was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the

requested amendment; is not part of the designated record set; would not be available for inspection; or is accurate and complete.

GLB
Not applicable.

5.2.3 Deadline
Not applicable.

5.2.4 Charges
Not applicable.

5.3 Erasure
5.3.1 Right
Not applicable.

5.3.2 Exceptions
Not applicable.

5.3.3 Deadline
Not applicable.

5.3.4 Charges
Not applicable.

5.4 Blocking
5.4.1 Right
Not applicable.

5.4.2 Exceptions
Not applicable.

5.4.3 Deadline
Not applicable.

5.4.4 Charges
Not applicable.

5.5 Objection
5.5.1 Right
Not applicable.

5.5.2 Exceptions
Not applicable.

5.5.3 Deadline
Not applicable.

5.5.4 Charges
Not applicable.

5.6 Automated individual decisions
5.6.1 Right
Not applicable.

5.6.2 Exceptions
Not applicable.

5.6.3 Deadline
Not applicable.

5.6.4 Charges
Not applicable.

5.7 Other rights
5.7.1 Right
Not applicable.

5.7.2 Exceptions
Not applicable.

5.7.3 Deadline
Not applicable.

5.7.4 Charges
Not applicable.

6. REGISTRATION OBLIGATIONS
Not applicable.

6.1 Notification requirements
Not applicable.

6.1.1 What
Not applicable.

6.1.2 Exceptions
Not applicable.

6.1.3 When
Not applicable.

6.1.4 How
Not applicable.

6.1.5 Notification fees
Not applicable.

6.2 Authorisation requirements
6.2.1 Who
Not applicable.

6.2.2 What
Not applicable.

6.2.3 Exceptions
Not applicable.

6.2.4 When
Not applicable.

6.2.5 How
Not applicable.

6.2.6 Authorisation fees
Not applicable.

6.3 Other registration requirements
None.

6.4 Register
Not applicable.

7. DATA PROTECTION OFFICER
FTCA
Not applicable.

HIPAA
Not applicable.

GLB
Various sections of GLB could be construed to require a data protection officer. For instance, the FTC's guidance provides that each financial institution must have an information security programme, and 'in order to develop, implement, and maintain your information security programme, you shall: (a) designate an employee or employees to coordinate your information security programme.'

7.1 Function recognised by law
FTCA
Not applicable.

HIPAA
Not applicable.

GLB
In order to develop, implement, and maintain the information security programme, the financial institution must: (i) designate the employee coordinator; (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorised disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the financial institution's operations; (iii) design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (iv) oversee service providers; and (v) evaluate and adjust the information security program in light of the results of the testing and monitoring.

7.2 Tasks and powers

FTCA
Not applicable.

HIPAA
Not applicable.

GLB
The employee coordinator would have the power to carry out and oversee all of the tasks listed in section 7.1 above.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Not applicable.

8.2 Legal basis for international data transfers

Not applicable.

8.2.1 Data transfer agreements

Not applicable.

8.2.2 Binding corporate rules

Not applicable.

8.2.3 Safe Harbour

The Safe Harbour scheme is a voluntary scheme under which US companies that are subject to the jurisdiction of the FTC or the Department of Commerce can self-certify in order to allow the transfer of personal data from the European Economic Area and Switzerland to the self-certified US

company. So far, more than 2,500 companies have signed up.

9. SECURITY OF DATA PROCESSING

FTCA

Section 5 does not set forth explicit standards regarding data processing. However, the FTC has traditionally used its unfairness and deception authority to bring enforcement actions where it has been alleged that data processing entities are subject to a heightened security burden. This may occur either as a result of specific representations to consumers regarding the entity's data security practices, or as a consequence of specific security standards imposed on the entity by applicable federal legislation (eg, GLB). More recently, however, the FTC has also exercised its unfairness authority in the security arena where it has been alleged that an entity lacked adequate information security measures, even when that entity is not subject to a heightened security burden for the aforementioned reasons.

HIPAA

Covered entities must ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and ensure compliance by its workforce. Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications.

GLB

Not applicable.

9.1 Confidentiality

FTCA

Not applicable.

HIPAA

Covered entities are obliged to ensure the confidentiality of data. Confidentiality means 'the property that data or information is not made available or disclosed to unauthorised persons or processes.'

GLB

Financial institutions are required to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records and to protect against unauthorised access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

9.2 Security requirements

FTCA

Despite the lack of explicit security requirements in Section 5 itself, the

FTC's enforcement actions clearly indicate that the FTC is willing to act in the security arena where it is alleged that: (i) data processing entities are subject to a heightened security burden; and (ii) they have failed to live up to that burden.

The principle means that a data processing entity may become subject to a heightened security burden by way of direct representations to consumers regarding the entity's information security practices. However, other federal laws may also subject data processing entities to heightened security burdens. For example, the FTC brought an enforcement action against Superior Mortgage Corporation, a financial institution that allegedly failed to comply with GLB's Safeguard Rule. Specifically, the FTC alleged that Superior Mortgage failed to: (i) assess risks to its customer information until more than a year after the Safeguard Rule became effective; (ii) institute appropriate password policies to control access to company systems and documents containing sensitive customer information; (iii) encrypt or otherwise protect sensitive customer information before sending it by email; and (iv) take reasonable steps to ensure that its service providers were providing appropriate security for customer information and addressing their own security risks in a timely and appropriate fashion. Importantly, the FTC specifically alleged that Superior Mortgage violated Section 5 by representing that personal information obtained from consumers online was encrypted at all times, when in fact such information: (i) was only encrypted while being transmitted between the visitor's web browser and the website service; and (ii) was decrypted and emailed to a number of offices in a clear, readable text once received by the company. This resulted in a settlement agreement that prohibited Superior from misrepresenting the extent of its data security safeguards and from violating the Safeguard Rule in the future.

More recent Section 5 enforcement actions suggest that the FTC is also willing to exercise its unfairness authority to regulate information security practices where the data processing entity is not subject to a particular heightened security burden. I*n the Matter of BJ's Wholesale Club, Inc., 042-3160 (F.T.C. 2005)* represents the first enforcement action in which the FTC relied exclusively on its unfairness authority and did not allege deceptive practices for misrepresentations of privacy or data security practices. This enforcement action arose after the FTC became aware that BJ's failed to use readily accessible security measures to protect personal information, including credit card numbers, which resulted in millions of dollars of fraudulent purchases. This conduct did not directly violate a federal statute, but the FTC concluded that the acts constituted an unfair business practice under Section 5.

HIPAA

Security or Security measures 'encompass all of the administrative, physical, and technical safeguards in an information system.'

Covered entities must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorised access is allowed.

A covered entity must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.

HIPAA also sets standards and implementations for technical safeguards which require the implementation of technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

Covered entities are also required to meet certain organisational requirements, which includes the entry of business associate agreements or other arrangements. This includes requirements that the business associate meet technical and security requirements, as well as many other requirements.

GLB

Financial institutions are required to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorised access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

9.3 Data security breach notification obligation

FTCA

Section 5 does not specifically obligate companies to notify affected individuals in the event of a data security breach, and the United States has yet to enact a federal breach notification law, despite the fact that such laws have been passed in 46 states (as of October 2011).

HIPAA

The HITECH Act requires that patients be notified of any unauthorised acquisition, access, use, or disclosure of their unsecured PHI that compromises the privacy or security of such information, though there are some exceptions related to unintentional or inadvertent disclosure by employees or authorised individuals with the 'same facility.'

GLB

There is no breach notification procedure under GLB, but there are state-specific breach notification laws in almost every state of the United States.

9.3.1 Who

FTCA

Not applicable.

HIPAA

The HITECH Act requires that patients be notified of any unauthorised acquisition, access, use or disclosure of their unsecured PHI that compromises the privacy or security of such information.

GLB

Not applicable.

9.3.2 What

FTCA

Not applicable.

HIPAA

The HITECH Act requires that patients be notified of any unauthorised acquisition, access, use or disclosure of their unsecured PHI that compromises the privacy or security of such information.

GLB

Not applicable.

9.3.3 To whom

FTCA

Not applicable.

HIPAA

The HITECH Act's notice requirements apply to patients.

GLB

Not applicable.

9.3.4 When

FTCA

Not applicable.

HIPAA

Notice given pursuant to the HITECH Act must be given 'promptly.'

GLB

Not applicable.

9.3.5 How

FTCA

Not applicable.

HIPAA

HITECH *'require[s] health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.'*

GLB

Not applicable.

9.3.6 Sanctions for non-compliance

FTCA

Not applicable.

HIPAA

The HITECH Act increases civil penalty amounts based upon the level of intent and neglect (ie, whether the violation was made without knowledge, due to reasonable cause, or due to wilful neglect). For violations determined to be made without knowledge, penalties start at $100 per violation, not to exceed $25,000. For violations based on reasonable cause, penalties start at $1,000 per violation, not to exceed $100,000. For violations due to wilful neglect, penalties start at $10,000, not to exceed $250,000. For violations due to wilful neglect that are not corrected, penalties start at $50,000, not to exceed $1.5 million.

GLB

Not applicable.

9.4 Data protection impact assessments and audits

FTCA

The FTC frequently includes a requirement that data processing entities conduct data protection impact assessments and allow the FTC to conduct audits in settlement agreements arising out of the FTC's enforcement authority. Although Section 5 does not contain any explicit requirement to this effect, entities that process personal data should consider it a best business practice to implement and maintain a written privacy and data security programme that addresses these issues.

HIPAA

The Secretary shall provide for periodic audits to ensure that covered entities and business associates comply with requirements.

GLB

GLB requires that, in accordance with a financial institution's information security programme, financial institutions must: *'identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorised disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the financial institution's operations.'*

9.4.1 Who

FTCA

Audit requirements may apply to entities that enter into settlement agreements with the FTC.

HIPAA
Covered entities must perform periodic technical and non-technical evaluations, based at least initially upon the standards implemented under HIPAA, and thereafter in response to environmental or operational changes affecting the security of electronic PHI. These evaluations must establish the extent to which an entity's security policies and procedures meet the requirements of HIPAA.

GLB
The financial institution.

9.4.2 What

FTCA
Generally, the FTC will require a respondent to establish and implement, and thereafter maintain, a comprehensive [written] privacy programme that contains privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the [personal information it collects]. One of the core requirements of such a programme is 'the evaluation and adjustment of respondent's privacy programme in light of any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy programme.'

HIPAA
Covered entities must perform periodic technical and non-technical evaluations.

GLB
Risk assessments must be a part of a financial institution's information security programme.

9.4.3 When

FTCA
The FTC generally stipulates that these obligations become effective as of the date the settlement agreement is served on the entity subject to a Section 5 enforcement action.

HIPAA
Covered entities must perform periodic technical and non-technical evaluations.

GLB
GLB does not set out a timeline for such risk assessments.

9.4.4 How

FTCA
Other than stipulating that the risk assessment must consider relevant

circumstances and that the privacy programme should be appropriate based on the respondent's size and the nature of its business operations, the FTC does not require a specific procedure for conducting such risks assessments.

HIPAA

Covered entities must: ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and ensure compliance from its workforce. Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement these standards.

GLB

Such risk assessments should be organised and conducted by the financial institution's employee coordinator for the information security programme.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

FTCA

The FTC essentially has two options regarding how to move forward once it has determined that an unfair or deceptive trade practice is occurring: (i) it may bring suit in federal court to obtain appropriate equitable relief - including restitution, discouragement, and either a temporary restraining order or a preliminary injunction pending the initiation of administrative action; or (ii) it may proceed exclusively in federal district court by filing a complaint seeking a permanent injunction and ancillary relief, including temporary or preliminary injunctive relief. Thus, in addition to injunctive relief the FTC can seek asset freezes, the appointment of a receiver, and discouragement or restitution of ill gotten gains. All remedies are available to the FTC with respect to unfair and deceptive acts or practices, including restitution to either domestic or foreign victims.

From a practical standpoint, however, FTC enforcement actions under Section 5 generally result in a settlement agreement that imposes numerous privacy, data security, administrative and reporting obligations on the data processing entity that allegedly engaged in unfair or deceptive business practices.

HIPAA

HHS may enter a resolution agreement if HHS believes that the covered entity requires corrective action. A resolution agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (eg, staff training) and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement likely would include

the payment of a resolution amount. These agreements are reserved to settle investigations with more serious outcomes. To date, HHS has entered into five resolution agreements.

GLB

In addition to enforcement by the FTC, similar to its FTCA enforcement powers, companies that do not comply with GLB can face actions by certain states who have made violation of GLB a violation of state law.

10.2 Sanctions

FTCA

Section 5 does not explicitly provide for sanctions for violating entities. However, all remedies are available to the FTC with respect to unfair and deceptive acts or practices, including restitution to either domestic or foreign victims.

HIPAA

Monetary sanctions are available for a violation of HIPAA. HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

Additionally, criminal penalties are also available. A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year in prison. The criminal penalties increase to $100,000 and up to five years in prison if the wrongful conduct involves false pretences, and to $250,000 and up to 10 years in prison if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm. The Department of Justice is responsible for criminal prosecutions under the Privacy Rule.

GLB

A knowing and intentional violation of certain portions of GLB is a felony that is subject to punishment of a fine or a prison term of up to five years, or both. If the activity involves more than $100,000 in a 12-month period, the fines can be doubled and the prison term can be up to 10 years.

10.3 Examples of recent enforcement of data protection rules

FTCA

The FTC regularly exercises its unfairness and deception authority and has initiated numerous enforcement actions under Section 5.

Several FTC enforcement actions indicate that the FTC views certain misrepresentations regarding a company's Safe Harbour certification status as a deceptive business practice. In order to be a participant in Safe Harbour, a company is required to self-certify with the US Department of Commerce that it complies with seven privacy principles and related requirements. In addition, companies are required to re-certify their Safe Harbour compliance annually to maintain 'current' Safe Harbour compliance status. The FTC has brought numerous enforcement actions where companies have represented that they are Safe Harbour compliant to consumers, when in fact such companies had either failed to re-certify or to become properly certified in the first place. These business practices are enforced under the FTC's Section 5 authority because Safe Harbour certification is essentially a representation that a given company maintains a certain level of privacy and data protection safeguards. In this sense, misstating one's Safe Harbour certification status is akin to making a false or deceptive representation about how one handles personal data.

HIPAA

In one recent incident a public hospital, in response to a subpoena (not accompanied by a court order), impermissibly disclosed the PHI of one of its patients. Contrary to the Privacy Rule protections for information sought for administrative or judicial proceedings, the hospital failed to determine that reasonable efforts had been made to ensure that the individual whose PHI was being sought received notice of the request and/or failed to receive satisfactory assurance that the party seeking the information made reasonable efforts to secure a qualified protective order. Among other corrective actions to remedy this situation, OCR required that the hospital revise its subpoena processing procedures. Under the revised process, if a subpoena is received that does not meet the requirements of the Privacy Rule, the information is not disclosed; instead, the hospital contacts the party seeking the subpoena and the requirements of the Privacy Rule are explained. The hospital also trained relevant staff members on the new procedures.

GLB

In February 2011, the FTC announced it settled charges with three companies whose business was reselling consumers' credit reports. The companies agreed to settle the FTC's charges that they did not take reasonable steps to protect consumers' personal information under the FCRA, FTCA and GLB, which failures allowed computer hackers to access that data. The FTC alleged that 'the resellers [ ] violated the [Safeguards Rule] by failing to design and implement information safeguards to control the risks to consumer information; to regularly test or monitor the effectiveness of their controls and procedures; to evaluate and adjust their information security programmes in light of known or identified risks; and to have comprehensive information security programmes.'

10.4 Judicial remedies

FTCA
All remedies are available to the FTC with respect to Section 5, including restitution to either domestic or foreign victims.

HIPAA
Litigation under HIPAA has been scarce. While certain individuals have tried to bring private claims for violations of HIPAA, courts have consistently held that no private right of action exists under this law. Thus, enforcement is largely left to the government agencies that have jurisdiction under HIPAA.

GLB
A knowing and intentional violation of certain portions of GLB is a felony that is subject to punishment of a fine or a prison term of up to five years, or both. If the activity involves more than $100,000 in a 12 month period, the fines can be doubled and the prison term can be up to 10 years.

10.5 Class actions

FTCA
Section 5 does not authorise class action lawsuits.

HIPAA
None. Enforcement is largely left to the government agencies that have jurisdiction under HIPAA.

GLB
One American court recently addressed the impact of GLB on class action discovery (Her v. Regions Financial Corp., 2007 WL 2806558 (W.D. Ark. 2007)). The plaintiff sought information including a list of people who received loans from the defendant. The court first concluded that the judicial process exception permitted disclosure of non-public information in response to interrogatories. It also concluded, given the fiduciary relationship of plaintiff's counsel that the fiduciary duty exception also permitted disclosure. However, the court did require that the borrowers' Social Security numbers, dates of birth, and drivers' licence numbers of the borrowers be redacted, although it found that prior notice to the borrowers was not required. This conclusion has been reached by a number of other courts, including state courts in New York.

10.6 Liability

FTCA
The data processing entity is generally liable for violations of Section 5. Although such violations typically give rise to individual legal claims under other state and federal laws, Section 5 does not allow individuals to claim damages.

HIPAA

The covered entity is responsible for any breach of HIPAA.

GLB

Individuals may not claim damages or enforce the GBL.

Contact details

GENERAL EDITOR

Monika Kuschewsky
Van Bael & Bellis
Avenue Louise 165
Brussels 1050
Belgium
T: +32 (0) 647 73 50
F: +32 (0) 2 640 64 99
E: mkuschewsky@vbb.com
W: www.vbb.com

FOREWORDS

Viviane Reding
European Commission Office
BERL 12/294
1049 Brussels
Belgium
Rue de la Loi
Wetstraat 200
1040 Brussels
T: +32-2-298.12.30
F: +32-2-299.92.01
E: martin.selmayr@ec.europa.eu
W: www.europa.eu

Peter Hustinx
European Data Protection Supervisor
Rue Wiertz, 60
B-1047 Brussels
Belgium
Office: rue Montoyer, 63, 6th floor
T: +32-2-283.19.00
F: +32-2-283.19.50
E: edps@edps.europa.eu
W: www.edps.europa.eu

Jean Gonié
Director of Privacy, EU Affairs
Microsoft Europe
Avenue des Nerviens, 85
B-1040 Brussels
Belgium
T: +32 (2) 704 3461
E: jgonie@microsoft.com
W: www.microsoft.com

AUSTRIA

Rainer Knyrim
Preslmayr
Dr Karl Lueger-Ring 12
1010 Vienna
Austria
T: +43 533 1695
F: +43 1535 5686
E: knyrim@preslmayr.st
W: www.preslmayr.at

BELGIUM

Monika Kuschewsky
Van Bael & Bellis
Avenue Louise 165
Brussels 1050
Belgium
T: +32 (0) 647 73 50
F: +32 (0) 2 640 64 99
E: mkuschewsky@vbb.com
W: www.vbb.com

CANADA

David Elder
Stikeman Elliott LLP
Suite 1600, 50 O'Connor Street
Ottawa, ON
K1P 6L2
T: +613 566 0532
E: delder@stikeman.com
W: www.stikeman.com

CYPRUS

Nicholas Ktenas
Chrystalla Neophytou
Andreas Neocleous & Co
Neocleous House
195 Makarios Avenue
PO Box 50613
Limassol

Cyprus, Cy 3608
T: +357 25 110000
F: +357 25 110001
E: ktenasn@neocleous.com
E: neophytou.chrystalla@neocleous.com
W: www.neocleous.com

CZECH REPUBLIC

Richard Otevřel
Havel, Holásek & Partners
Týn 1049/3
Prague 110 00
Czech Republic
T: +420 224 895 950
F: +420 224 895 980
E: richard.otevrel@havelholasek.cz
W: www.havelholasek.cz

DENMARK

Johnny Petersen
Delacour Dania
Langebrogade 4
Copenhagen K
Denmark
DK-1411
T: +45 7011 1122
F: +45 7011 1133
E: jp@delacourdania.dk
W: www.delacourdania.dk

EU

Monika Kuschewsky
Van Bael & Bellis
Avenue Louise 165
Brussels 1050
Belgium
T: +32 (0) 647 73 50
F: +32 (0) 2 640 64 99
E: mkuschewsky@vbb.com
W: www.vbb.com

FRANCE

Raphaël Dana
Ramiro Tavella
47 avenue Hoche
Paris 75008
France
T: +33 1 47 63 45 63
E: r.dana@sarrut-avocats.com
W: www.sarrut-avocats.com

GERMANY

Monika Kuschewsky
Van Bael & Bellis
Avenue Louise 165
Brussels 1050
Belgium
T: +32 (0) 647 73 50
F: +32 (0) 2 640 64 99
E: mkuschewsky@vbb.com
W: www.vbb.com

HUNGARY

János Tamás Varga
Zoltán Tarján
VJT & Partners Law Firm
Kernstok Károly tér 8
1126 Budapest
Hungary
T: +36 1 501 9900
F: +36 1 501 9901
E: vargajt@vjt-partners.com
E: tarjanz@vjt-partners.com
W: www.vjt-partners.com

INDIA

Naheed Carrimjee
Desai, Desai Carrimjee & Mulla
2A/2B, Jeevan Jyot
2nd Floor
18/20, Cawasji Patel Street
Fort, Mumbai – 400 001
India
T: +91-22-22819901
F: +91-22-22819910
E: naheed.carrimjee@ddcm.in
W: www.ddcm.in

IRELAND

Aoife Treacy
Mason Hayes & Curran
South Bank House
Barrow Street

Dublin 4
Ireland
T: +353 1 614 5000
F: +353 1 614 5001
E: atreacy@mhc.ie
W: www.mhc.ie

ISRAEL

Yoheved Novogroder-Shoshan
Yigal Arnon & Co
22 Rivlin Street
Jerusalem 94240
Israel
T: +972 2 623 9200
F: +972 2 623 9236
E: yohevedn@arnon.co.il
W: www.arnon.co.il

ITALY

Gerolamo Pellicanò & Giovanna Boschetti
CBA Studio Legale e Tributario
Galleria San Carlo, 6
Milan 20122
Italy
T: +39 02 778061
F: +39 02 76007900
E: gerolamo.pellicano@cbalex.com
E: giovanna.boschetti@cbalex.com
W: www.cbalex.com

LATVIA

Linda Lejina & Ilze Bukaldere
BORENIUS
Lacplesa 20a
Riga 1011
Latvia
T: +371 67201800
F: +371 67201801
E: linda.lejina@borenius.lv
E: ilze.bukaldere@borenius.lv
W: www.borenius.lv

LUXEMBOURG

Héloïse Bock
Arendt & Medernach
14, rue Erasme L-2082
Luxembourg
T: +352 40 78 78 321
F: +352 40 78 04 695
E: heloise.bock@arendt.com
W: www.arendt.com

MALTA

Michael Zammit Maempel & Mark Hyzler
GVTH Advocates
192 Old Bakery Street
Valletta, VLT 1455
Malta
T: +356 212 2888
F: +356 212 2808
E: michael.zammitmaempel@gvthlaw.com
E: mark.hyzler@gvthlaw.com
W: www.gvthlaw.com

MEXICO

Laura Collada & Jorge Molet
Dumont Bergman Bider & Co., S.C.
Av. de los Insurgentes Sur 1898, piso 21, Colonia Florida.
Mexico City 01030
Mexico
T: +52 (55) 53226230
F: +52 (55) 56613056
E: lcollada@dumont.com.mx
E: jmolet@dumont.com.mx
W: www.dumont.com.mx

NETHERLANDS

Polo van der Putt & Eva de Vries
Vondst Advocaten
Jacob Obrechtstraat 56
Amsterdam 1071 KN
The Netherlands
T: +31 (0)20 504 2000
F: +31 (0)20 505 2010
E: polo.vanderputt@vondst-law.com
E: eva.devries@vondst-law.com
W: www.vondst-law.com

POLAND

Agata Szeliga
Sołtysiński, Kawecki & Szlęzak

ul. Wawelska 15 B
02-034 Warsaw Poland
T: +48-22 608 7000
F: +48-22 608 7070
E: agata.szeliga@skslegal.pl
W: www.skslegal.pl

PORTUGAL

Mónica Oliveira Costa
Coelho Ribeiro e Associados – Sociedade Civil de Advogados, R.L
Av. Eng.º Duarte Pacheco
Empreendimento das Amoreiras
Torre II, 13.ºA
Lisbon 1099-042
Portugal
T: +351 21 383 9060
F: +351 21 385 3202
E: monica.costa@cralaw.com
W: www.cralaw.com

ROMANIA

Roxana Ionescu & Ovidiu Balaceanu
Nestor Nestor Diculescu Kingston Petersen
Bucharest Business Park
1A Bucuresti-Ploiesti National Road
Entrance A, 4th Floor, 1st District
Bucharest 013681
Romania
T: +40 21 201 1200
+40 31 225 3300
F: +40 21 201 1210
+40 31 225 3310
E: roxana.ionescu@nndkp.ro
E: ovidiu.balaceanu@nndkp.ro
W: www.nndkp.ro

SLOVAKIA

Richard Otevřel & Jaroslav Šuchman
Havel, Holásek & Partners
Týn 1049/3
Prague 110 00
Czech Republic
T: +420 224 895 950
F: +420 224 895 980
E: richard.otevrel@havelholasek.cz
E: jaroslav.suchman@havelholasek.cz
W: www.havelholasek.eu

SOUTH AFRICA

André Visser & Danie Strachan
Adams & Adams
Lynnwood Bridge
4 Daventry Street
Lynnwood Manor
P O Box 1014
Pretoria 0001
South Africa
T: +27 12 432 6000
F: +27 12 432 6599
E: AV@adamsadams.co.za
E: danie-s@adamsadams.co.za
W: www.adamsadams.co.za

SPAIN

Cecilia Álvarez Rigaudias & Leticia López-Lapuente
Uría Menéndez
Príncipe de Vergara 187
Madrid 28002
Spain
T: +34 915860400
F: +34 915860617
E: cia@uria.com
E: lll@uria.com
W: www.uria.com

SWEDEN

Erica Wiking Häger, Mikael Moreira & Anna Nidén
Mannheimer Swartling
Norrlandsgatan 21
PO Box 1711
111 87 Stockholm
Sweden
T: +46 8 595 060 00
F: +46 8 595 060 01
E: ewh@msa.se
E: mma@msa.se
E: anni@msa.se
W: www.mannheimerswartling.se

SWITZERLAND

Lukas Morscher & Martin Vonaesch
Lenz & Staehelin
Bleicherweg 58
8027 Zurich
Switzerland
T: +41 58 450 80 00
F: +41 58 450 80 01
E: lukas.morscher@lenzstaehelin.com
E: martin.vonaesch@lenzstaehelin.com
W: www.lenzstaehelin.com

TURKEY

Gönenç Gürkaynak, İlay Yılmaz &
Ceren Yıldız
ELIG
Çitlenbik Sokak, No:12
Yıldız Mahallesi 34349
Beşiktaş, Istanbul
Turkey
T: +90 212 327 17 24
F: +90 212 327 17 25
E: gonenc.gurkaynak@elig.com
E: ilay.yilmaz@elig.com
E: ceren.yildiz@elig.com
W: www.elig.com

UK

Hazel Grant & Mark Watts
Bristows
100 Victoria Embankment
London EC4Y 0DH
UK
T: +44 (0)20 7400 8000
E: hazel.grant@bristows.com
E: mark.watts@bristows.com
W: www.bristows.com

USA

Andrew Serwin & Daniel Muto
Megan O'Sullivan
Foley & Lardner LLP
3579 Valley Centre Drive
Suite 300 San Diego
CA 92130-3302
USA
T: +858 847 6700
F: +858 792 6773
E: aserwin@foley.com
E: dmuto@foley.com
E: mosullivan@foley.com
W: www.foley.com