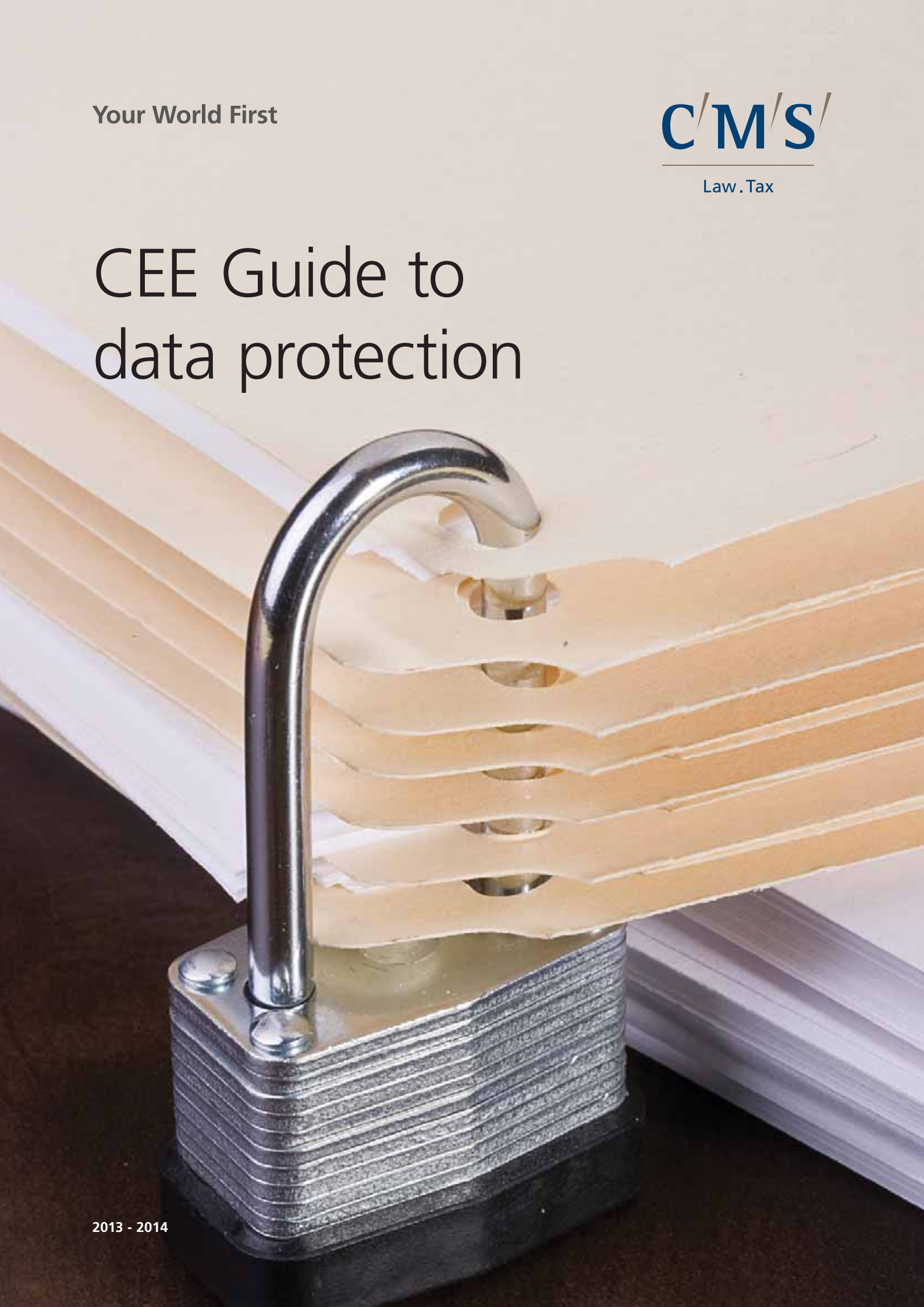
Your World First

C/M/S/
Law.Tax

CEE Guide to data protection



2013 - 2014


Aberdeen
Edinburgh
Moscow
Hamburg
Amsterdam
Berlin
Warsaw
London
Utrecht
Duesseldorf
Leipzig
Bristol
Antwerp
Dresden
Cologne
Kyiv
Brussels
Frankfurt
Prague
Luxembourg
Vienna
Paris
Stuttgart
Strasbourg
Munich
Bratislava
Zurich
Budapest
Lyon
Ljubljana
Zagreb
Milan
Belgrade
Bucharest
Sarajevo
Sofia
Barcelona
Rome
Tirana
Istanbul
Madrid
Lisbon
Seville
Algiers
Casablanca
Dubai
Mexico City
Beijing
Shanghai
Rio de Janeiro

Introduction

The importance of data protection law in Central and Eastern Europe
When planning business operations in Central and Eastern Europe (CEE), data protection law is as important as any other area of law. Most business projects will involve some processing of personal data, whether that of employees, customers or potential clients. In fact, personal data protection rules will potentially apply in any scenario where information relating to an individual is involved in any way.

How to use this guide
We have prepared this guide to data protection in Central and Eastern Europe with the aim of providing an overview of the various national personal data protection frameworks that exist in CEE. The guide contains practical information on the scope, rules and enforcement consequences of the personal data protection frameworks in the following jurisdictions, listed alphabetically: Bulgaria, the Czech Republic, Hungary, Poland, Romania, the Russian Federation, Slovakia and Ukraine.

CMS Cameron McKenna has provided legal assistance in each of these jurisdictions for many years. For your convenience, the guide has been structured in a question and answer format. Drawing on our extensive experience in handling personal data protection matters across the region, we have selected questions that we believe you should be asking when planning, implementing or evaluating personal data protection policies. The guide is divided into chapters, each of which answers similar questions in respect of a different jurisdiction. Please note that the guide and its contents do not constitute legal advice. Professional legal advice should be sought when navigating through any data protection issues. The contents of the guide are correct as at 1 October 2013.

CMS Cameron McKenna's CEE Data Protection Group
All of our CEE offices have dedicated data protection lawyers. This puts our firm in the advantageous position of being able to advise on data protection issues across the region. Through the CMS Cameron McKenna CEE Data Protection Group, our internal forum for knowledge-sharing and training in this area of the law, our lawyers communicate regularly to tackle client issues and discuss current legal developments. We hope that the guide is of practical assistance to you and that you enjoy using it. Please contact us if you require any further information.

Iain Batty
CEE Head of Commercial, Regulatory and Disputes
T +48 22 520 5528
E iain.batty@cms-cmck.com

Dóra Petrányi
CEE Head of Privacy Initiative
T +36 1 483 4820
E dora.petranyi@cms-cmck.com

Bulgaria

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?
The Bulgarian Data Protection Act dated 4 January 2002, as amended ('Data Protection Act') implements Directive 95/46/EC into Bulgarian legislation.

The Data Protection Act defines personal data and data processing, regulates consent rules, data transfer, the obligations of data processors and the rights and remedies of relevant persons. Other sector-specific laws and by-laws may also be applicable depending on the case.

The Data Protection Act applies to the processing of personal data where the data controller:
(a) is established in the territory of the Republic of Bulgaria
(b) is not established in the territory of the Republic of Bulgaria but must apply the Data Protection Act by virtue of international public law
(c) is not established in the territory of the EU or the European Economic Area (EEA), but, for the purposes of such processing, makes use of means located in the territory of the Republic of Bulgaria (unless such means are being used exclusively for transit purposes).

2. What is the data privacy authority (DPA) in your country?
The supervisory authority established in accordance with Article 28 of Directive 95/46/EC is the Bulgarian Data Protection Commission (*Комисия за Защита на Личните Данни („КЗЛД" or 'DPA'*). Its website can be found at www.cpdp.bg/en/index.php?p=home&aid=0.

3. Does an internal data privacy officer or similar need to be appointed?
No. Such appointment is voluntary.

4. Do most companies have internal privacy policies and external privacy notices?
Yes, in our experience most international companies active on the market have internal policies for personal data protection as well as internal rules for the protection of databases. The Data Protection Act expressly provides that industry-specific data protection codes of ethics may also be prepared.

5. What is deemed as 'personal data'?
The Data Protection Act is similar to Directive 95/46/EC in that it does not provide for an exhaustive list of data which is deemed as 'personal data'. Thus 'personal data' is assessed on a case-by-case basis. 'Personal data' means any information relating to a natural person identified or identifiable directly or indirectly, in particular by reference to an identification number or to one or more specific features.

In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ('sensitive personal data') which may not be collected without consent, i.e. personal data revealing (a) racial or ethnic origin, or political, religious or philosophical beliefs, (b) membership of political parties or organisations, associations with religious, philosophical, political or trade-union bodies, and (c) health, sex life, or human genome.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?

In some cases it may be necessary to obtain the prior express consent of data subjects in order to collect and transfer their personal data. It is advisable to obtain it even when it is not mandatory.

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?

On the basis of Article 7 (c) and (f) of Directive 95/46/EC, personal data can be processed when it is necessary for:

(a) compliance with a legal obligation applicable to the data processor
(b) the fulfilment of obligations under an agreement to which the individual to whom such data relates is party, as well as for any activities initiated by the same individual prior to the conclusion of the agreement
(c) the protection of the life and health of the individual to whom the data relates
(d) the performance of a task carried out in the public interest
(e) the exercise of an official authority vested by law in the processor or in a third party to whom the data is disclosed
(f) the realisation of the legitimate interests of the data processor or a third party, except where such interests are overridden by the interests of the individual to whom the data relates.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?

The transfer of data to an EU/EEA member state is treated the same as data transferred within the territory of Bulgaria.

Personal data may be transferred to a third country only if the third country ensures an adequate level of protection, where adequacy is evaluated by the DPA unless EC Model Clauses are used.

In addition to the above, a data controller may transfer data if:

(a) the relevant person has provided consent
(b) the transfer is required for the fulfilment of obligations under an agreement between the data controller and the relevant person – for the execution and performance of the obligations under an agreement signed in the best interests of the data subject (where the agreement is signed for the benefit of the data subject) by the data controller and a third party
(c) the transfer is required by law or important public interest, or for the establishment, exercise or defence of legal claims or the transfer is necessary in order to protect the life and health of the individual to whom such data relates.

In practice, the DPA adopts quite a restrictive approach with respect to the transfer of personal data and requires a notification in case of transfer outside the EEA. It is advisable to make a notification of any data transfer to a third country. Approval is required in the cases provided for by the Data Protection Act.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?

A group company is regarded as a third party, and, as above, would either (a) need to independently satisfy the legal requirements for processing personal data, or (b) the data privacy consent provided to the 'original' data controller must contain consent to the processing/transfer between the group companies, and the relevant companies should enter into a written data transfer agreement in order to ensure compliance with the data transfer obligations stated above.

10. When collecting personal data, what information needs to be given, and how?

The Data Protection Act has strictly implemented the requirements listed in Section IV (*Information to be given to the relevant person*) of Directive 95/46/EC as follows: Before the commencement of data processing the relevant person must be given clear and detailed information on all circumstances in relation to the data processing, including:

(a) the identity of the controller and its representative, if any
(b) the purposes of the data processing
(c) the recipients or categories of recipients of the data
(d) whether providing the data is mandatory or voluntary, as well as the possible consequences of failing to provide the data
(e) the existence of the right of access to and the right to rectify the data concerning him/her.

The Data Protection Act also implements the requirements under Section V (*The Relevant Person's Right of Access to Data*) and provides the relevant person with the right to request at any time and without cost:

(a) confirmation on whether or not data relating to such person is being processed and information on at least the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed

(b) communication in an intelligible form of the data undergoing processing and of any available information as to its source
(c) knowledge of the logic involved in any automatic processing of data concerning the person at least in the case of automated decisions.

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?
We recommend translation into Bulgarian in order to ensure compliance with the requirement for communication in an intelligible form of the data undergoing processing and of any available information.

12. What are the specific rules where the data controller has appointed a third party to process personal data?
Controllers may process data themselves or assign it to data processors. When this is required for organisational reasons, processing may be assigned to more than one data processor and their specific tasks defined.

Where data processing is not performed by the controller, the controller designates a data processor/processors and provides sufficient data protection guarantees. Under Bulgarian law it is possible for a processor/processors to process data alone, without the controller doing any processing.

The relationship between the controller and the processor must be governed by a legal act, by a written contract or other act that defines the scope of duties assigned by the controller to the processor. The controller is jointly and severally liable with the processor for any damage caused to any third party resulting from any action or failure to act by the data processor.

A personal data processor or any person acting under the guidance of the controller or the processor who has access to personal data may process them only on instructions from the controller, unless otherwise provided for by law.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?
In line with Article 6 of Directive 95/46/EC, personal data may be processed to the extent and for the duration necessary to achieve the purpose of the processing. Any document containing personal data must be destroyed as soon as its purpose is served unless the data is transferred to another data controller after notification to the DPA if the transfer is required by law and the purpose of the processing is identical. Storage is permitted – if the purpose of the processing has been achieved – only if provided for by law (e.g. storage as anonymous data). (This notification is not related to transfers to non-EU countries. It is mandatory in the case of transfer to another controller when the purpose of the data collection has been achieved and if the transfer is provided by law.)

This question should be assessed on a case-by-case basis.

14. Specify below the mandatory technical, organisational or security measures.
The Data Protection Act implements the provisions of Section VIII of Directive 95/46/EC (*Confidentiality and Security of Processing*). The 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 processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Specific measures should be undertaken in the case of transfer of data by electronic means.

The measures above must comply with the technological progress and ensure protection complying with the risks and type of data to be protected. The minimal level of technical and organisational measures are subject to a specific ordinance ('*Ordinance No. 1 dated 7 February 2007 for the minimal level of technical and organisational measures and allowed type of protection of personal data*').

15. Does a data controller have any other specific obligations?
There are no other specific obligations listed in the Data Protection Act.

16. What are the registration obligations at the DPA?
In accordance with Article 18 of Directive 95/46/EC, data controllers must register with the DPA prior to carrying out any data processing activities. This involves completing the DPA's standard online or paper application form. Data processing can commence at the moment the application is filed. The DPA registers the controller within 14 days.

The data controller must inform the DPA of any change in the data provided in the application form in advance, unless the change is required by law (where the DPA must be notified of the amended data within seven days of the new law coming into effect).

The online Data Protection Registry is available for inspection at the following address: 212.122.176.6:8081/CPDP_ERALD/pages/publicRegisters/confirmedPublicRegisterList.faces

17. Are there any exemptions from the registration obligation?
Registration is not required if:
(a) the data controller maintains a register which, by virtue of a legal provision, is intended for public information and access to it is free, or access to it is granted to a person with a legal interest
(b) the data processor is a non-profit organisation under specific conditions.

The DPA may also waive the registration obligation – if requested upon application – if the processing does not infringe the rights and legitimate interests of the individuals whose data is being processed.

18. Are there any specific notification obligations?
There are no specific notification obligations. However, it is advisable to consider on a case-by-case basis whether additional notifications should be sent to the DPA. The DPA closely controls the correct and compliant processing of personal data in Bulgaria.

19. Does the relevant person have the right to access, rectify, remove or block their personal data?
The data processor must comply with the data subject's right to rectify, delete or block data which is processed not in compliance with the provisions of the Data Protection Act and to inform third parties to whom personal data was disclosed about such rectification, deletion or blocking. In addition to this, a data subject has the right to access his/her personal data through a written application to the data collector (online application is also possible) and to receive oral or written information on the data processing.

A data subject also has the right:
(a) to object to the controller with regard to the processing of his or her personal data on the basis of legitimate grounds; where such objection is justified, the individual's personal data may no longer be processed
(b) to object to the processing of his or her personal data for the purposes of direct marketing
(c) to be informed before his or her personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be given the opportunity to object to such disclosure or use.

The data collector must inform the data subject about these rights.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?
(A) Administrative remedies and other sanctions

If the provisions of the Data Protection Act are violated, the DPA is entitled to:
(a) order a temporary prohibition on processing personal data
(b) provide mandatory recommendations that must be immediately observed by the data controller
(c) remove the data controller from the Data Protection Registry
(d) impose a fine of up to BGN 100,000 (approximately €50,000) and to double this amount in the case of recurring offences.

In order to decide whether a fine is justified and to determine the amount of the fine, the DPA will take into account all the circumstances of the case, including the range of persons affected by the violation of the law, and the gravity or repeated nature of the violation.

(B) Judicial remedies
In accordance with Article 22 of Directive 95/46/EC (*Remedies*), the Data Protection Act provides that the relevant person may file for a court action against the controller.

(C) Criminal Liability
Under Bulgarian Law only individuals can be subject to criminal liability. Unlawful activity related to personal data may result in such criminal liability in some specific cases.

Czech Republic

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?
In the Czech Republic, general data privacy is regulated by Act No. 101/2000 Coll., the Data Protection Act ('Data Protection Act'). The Data Protection Act is based on Directive 95/46/EC and sets a general framework for data protection. It defines personal data and data processing, regulates consent rules, data transfer, the obligations of data processors and the rights and remedies of the relevant persons. An unofficial English translation of the Data Protection Act can be found here: www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en.

There are also several laws which contain sector-specific privacy and security requirements.

The Data Protection Act applies to all processing of the data of natural persons in the territory of the Czech Republic. It is assumed that the Data Protection Act also applies to any disclosure or export of personal data collected in the Czech Republic, even if the data are disclosed or exported outside the Czech Republic. The Data Protection Act also applies if the law of the Czech Republic is applicable on the basis of international public law, even if the controller is not established in the Czech Republic, and if a controller established outside the territory of the European Union carries out processing in the territory of the Czech Republic, unless the processing concerns the transfer of personal data within the territory of the European Union. In this case the controller is obliged to authorise a processor in the Czech Republic.

2. What is the data privacy authority (DPA) in your country?
The supervisory authority established in accordance with Article 28 of Directive 95/46/EC is the Czech Data Protection Authority (*Úřad pro ochranu osobních údajů*). Its website can be found at www.uoou.cz/uoou.aspx?lang=en.

3. Does an internal data privacy officer or similar need to be appointed?
In general, there is no statutory duty to appoint a data privacy officer. Appointing a person responsible for adhering to the data protection legislation is, however, a frequent market practice.

4. Do most companies have internal privacy policies and external privacy notices?
Yes, in our experience, this is a good market practice that many companies observe.

5. What is deemed as 'personal data'?
The Data Protection Act is similar to Directive 95/46/EC in that it does not provide for an exhaustive list of data which is deemed as 'personal data'. Thus 'personal data' is

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

In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ('sensitive personal data') which means personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sex life, and genetic data; sensitive data also means biometric data permitting direct identification or authentication of the relevant person.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?

A controller may process personal data only with the consent of the relevant person. Without such consent, the controller may process the data only in cases explicitly stated in the Data Protection Act (please refer to question 7 below).

In practice, consent can be given verbally, in writing, electronically or by implication. Electronic acceptance may be acceptable through – for example – a click by the relevant person on an 'acceptance button' or 'consent box'. Before ticking, the relevant person should also be given an opportunity to read the relevant privacy policy, which gives information on the data processing.

The controller must be able to prove that the relevant person has given consent to the personal data processing for the whole period of the processing. For this reason, it is in most cases recommended to obtain consent in writing.

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?

Personal data can be processed without the relevant person's consent if the data processor meets one of the following conditions:

(a) if the processing is essential to comply with the controller's legal obligation (e.g., an employer processing personal data of its employees in the necessary extent)
(b) if the processing is essential for the fulfilment of a contract to which the relevant person is a contracting party or for negotiations on concluding or altering a contract negotiated on the proposal of the relevant person
(c) if it is essential for the protection of vitally important interests of the relevant person. In this case, the consent of the relevant person must be obtained later without undue delay. If the consent is not granted, the controller must terminate the processing and destroy the data
(d) in relation to personal data that were lawfully published in accordance with special legislation (e.g., data published in the Czech Commercial Register). However, this will not prejudice the right to the protection of the private and personal life of the relevant person
(e) if it is essential for the protection of the rights and legitimate interests of the controller, recipient or other person concerned. However, such personal data processing may not be in contradiction with the right of the relevant person to protection of his private and personal life
(f) if it affects 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
(g) if the processing relates exclusively to archival purposes pursuant to Czech archiving regulations.

In the case of sensitive data, the regulation is even stricter. Without the relevant consent, the data processor may process sensitive data only in the following cases:

(a) if it is necessary to preserve the life or health of the relevant person or some other person or to eliminate imminent serious danger to their property, if his/her consent cannot be obtained, in particular, due to physical, mental or legal incapacity, or if the relevant person is missing, or for similar reasons. The controller is obliged to terminate data processing as soon as the above reasons cease to exist and must destroy the data, unless the relevant person gives consent to further processing
(b) if the processing in question involves ensuring health care, public health protection, health insurance, and the exercise of public administration in the health sector, or it is related to an assessment of health
(c) if the processing is necessary due to the obligations and rights of the data controller in the fields of labour law and employment
(d) if the processing is for political, philosophical, religious or trade-union aims and is carried out within the scope of legitimate activity of a civil association, foundation or other non-profit legal person (hereinafter referred to as the 'association') and which relates only to members of the association or persons with whom the association is in frequent contact related to legitimate activity of the association, and the personal data are not disclosed without the consent of the relevant person
(e) if the data processed are necessary for sickness insurance, pension insurance (security), accident insurance, state social support and other state social security benefits, social services, social care, assistance in material needs and the social and legal protection of children, and if, at the same time, the protection of the data is ensured in accordance with the law

(f) if the processing concerns personal data published by the relevant person
(g) if the processing is necessary to secure and exercise legal claims
(h) if they are processed exclusively for archival purposes
(i) if the processing is performed under special acts regulating the prevention, investigation or detection of criminal activities, prosecution of criminal offences and searches for persons.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?
The transfer of personal data to other EU countries is not restricted.

Personal data may be transferred freely to non-EU countries where the transfer is required or allowed by national law, by the provisions of a ratified international treaty, or on the basis of a decision of an EU institution (i.e. EC Model clauses). If none of these cases apply, then the transfer may only take place after the DPA has been notified and has issued authorisation for the transfer. In most cases, the DPA must issue such authorisation within 30 days.

Such a transfer may only take place provided that at least one of the below conditions are fulfilled:
— The transfer is carried out with the consent of, or on the basis of an instruction from, the relevant person.
— The laws of the country of destination ensure an adequate level of data protection.
— The personal data is kept in publicly accessible data files, as provided for by specific legislation, or is accessible to anyone who proves sufficient legal interest.
— The transfer is held to be in the public interest, as provided for by specific legislation, or by an international treaty binding on the Czech Republic.
— The transfer is necessary for negotiating the conclusion or change of a contract, carried out at the relevant person's request, or for the performance of a contract to which the relevant person is a contracting party.
— The transfer is necessary to perform a contract between the data controller and a third party, concluded in the interest of the relevant person, or to exercise other legal claims.
— The transfer is necessary for the protection of the rights or vital interests of the relevant person, in particular for preventing death or providing health care.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?
The Data Protection Act does not acknowledge holding companies as a specific subject of regulation; therefore no different regulation applies.

10. When collecting personal data, what information needs to be given, and how?
The data collector must provide the relevant person with information on the scope in which and the purpose for which the personal data is to be processed, who will process the personal data and in what manner, and to whom the personal data may be disclosed. This does not apply only if the relevant person is already aware of this information. The controller must also inform the relevant person about his/her right of access to personal data, the right to have the personal data rectified as well as other rights provided for in the Data Protection Act.

Although the Data Protection Act does not require the information to be provided in written form, it is advisable to do so.

If the data controller processes personal data obtained from the relevant person, it is obliged to tell the relevant person whether the provision of the personal data is mandatory or voluntary. As a result of this, it should be ascertained that the relevant person knows whether he/she has the right to refuse to provide the data to the data controller.

The controller is not obliged to provide the information described above if the personal data were not obtained from the relevant person (e.g. the data were received from publicly available sources), if
(a) it is processing personal data exclusively for the purposes of the state statistical service, scientific or archival purposes and the provision of such information would involve a disproportionate effort or inadequately high costs; or if storage on data carriers or disclosure is expressly provided by a special act. In these cases the controller is obliged to take all necessary measures against unauthorised interference with the relevant person's private and personal life
(b) the personal data processing is imposed on him by a special act or such data are necessary to exercise the rights and obligations ensuing from special acts
(c) it is processing exclusively lawfully published personal data (e.g. from the Commercial Register)
(d) it is processing personal data obtained with the consent of the relevant person (e.g. if the relevant person gave his/her consent to a data controller to transfer the data to the data controller in question).

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?
The Data Protection Act does not specify the language of the notices and consents in connection with data processing, so the English language may be deemed sufficient. It is not mandatory to translate such documents into the local language if the relevant person has good command of English. As Czech versions of all documents may be required, e.g. in the course of any administrative or court proceedings, it is recommended to produce bilingual documents.

12. What are the specific rules where the data controller has appointed a third party to process personal data?
The data controller may authorise a third party to process personal data. Where such authorisation does not follow from a legal regulation, the controller must conclude an agreement on personal data processing with the processor. The agreement must be made in writing. In particular, the agreement must explicitly stipulate the scope, purpose and period of time for which it is concluded and must contain guarantees from the processor related to the technical and organisational protection of the personal data.

If a third party data processor is appointed, it must adhere to all the data controller's legal obligations under the Data Protection Act.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?
Personal data may be processed to the extent and for the duration necessary to achieve the purpose of the processing. As soon as there is no further legitimate reason to retain the personal data, they must be destroyed.

As regards specific archiving rules, it is advisable to retain data until the end of the relevant period of limitation. In civil and employment law matters, the period of limitation is three years. In commercial matters, the period of limitation is four years. In specific cases, there may be different rules for the limitation periods.

In addition, there are several laws which prescribe a specific retention period for some types of document. As an example, a longer retention period may apply to documents relating to payment of taxes and social security contributions or to accounting documents. A specific retention period is also envisaged for records relating to duties under the Czech anti-money-laundering legislation. Any concerns regarding the retention obligation pertaining to a particular document are assessed on a case-by-case basis.

14. Specify below the mandatory technical, organisational or security measures.
Section 13 of the Data Protection Act implements the provisions of Section VIII of Directive 95/46/EC (*Confidentiality and Security of Processing*).

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

In addition, the data controller or the data processor are obliged to develop, implement and document technical and organisational measures to ensure that personal data is protected in accordance with the law and other legal regulations. The Data Protection Act does not provide further details on the technical and organisational measures mentioned above.

Furthermore, under the Data Protection Act the data controller or the data processor must perform a risk assessment concerning the following:
(a) the provision instructions for personal data processing by persons who have immediate access to the personal data
(b) the prevention of unauthorised people from accessing personal data and the means for their processing
(c) the prevention of unauthorised reading, creating, copying, transferring, modifying or deleting of records containing personal data and
(d) measures to determine and verify to whom the personal data were transferred.

Such a risk assessment should always be performed; the complexity of the process will depend upon the sector and type of activity performed by the data controller or the data processor. Written documents should be kept in order to evidence that the risk assessment was carried out properly. The DPA has not produced any template documents or other detailed guidelines yet on how it should be done.

The failure to undertake such risk assessment itself should not lead to sanctions; however, if the DPA concludes that a company has not adopted sufficient measures for the protection of the personal data, a fine of up to CZK 5,000,000 (approx. €200,000) can be imposed.

15. Does a data controller have any other specific obligations?
As an example, a data controller must ensure that its employees, other contractors or other persons who come into contact with personal data at the controller's premises keep the personal data strictly confidential. This obligation survives the termination of cooperation with the data controller.

16. What are the registration obligations at the DPA?
In general, before it starts to collect personal data, a data controller must notify the DPA.

The notification must include the following information:
(a) the identification data of the controller
(b) the purposes of processing
(c) the categories of the persons affected and of the personal data pertaining to these subjects
(d) the sources of personal data
(e) a description of how the personal data will be processed
(f) the location or locations of personal data processing
(g) the recipient or category of recipients
(h) the anticipated personal data transfers to other countries
(i) a description of the technical and organisational measures adopted for ensuring the protection of personal data.

The registration can be done through an electronic form available on the website of the DPA. If the application fulfils all statutory requirements, it will be accepted by the DPA within a statutory period of 30 days (in practice, this usually takes approx. one week). After the expiry of the statutory period, the data collection may commence.

17. Are there any exemptions from the registration obligation?
Registration in the Data Protection Registry is not necessary if:
(a) the personal data are part of data files which are publicly accessible on the basis of a special act (e.g. data accessible in the Commercial Register)
(b) the processing is imposed on the controller by a special act or when such personal data are needed for exercising rights and obligations following from a special act (e.g. some personal data of employees processed by an employer) or
(c) the processing is for political, philosophical, religious or trade- union aims carried out within the scope of the 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 association's legitimate activity, and the personal data are not disclosed without the consent of the relevant person (e.g. some personal data of members of a political party processed by the political party).

18. Are there any specific notification obligations?
There is a specific notification obligation in the case of data transfer to third countries (please refer to point 8 above).

19. Does the relevant person have the right to access, rectify, remove or block their personal data?
In line with Article 12 (*Right of access*) of Directive 95/46/EC, the Data Protection Act stipulates that the relevant person has the following rights:

Information
If the relevant person requests information on the processing of his personal data, the data controller must provide him with this information without undue delay.

The relevant person must always be informed of the following points:

(a) the purpose of processing the personal data
(b) the personal data or categories of personal data that are subject to processing including all available information on their source
(c) the character of automated processing in relation to its use for decision making, if acts or decisions are taken on the basis of the processing which may interfere with the relevant person's rights and legitimate interests
(d) the recipients or categories of recipients.

In terms of payments, the data controller is only entitled to require a reasonable reimbursement not exceeding the costs necessary for the provision of information. Such reimbursement should not exceed the costs that the data controller has had in connection with the provision of information.

Rectification

Data processors must rectify all personal data if it is false.

Deletion

This option arises only if a person finds or presumes that a controller or processor is processing his/her personal data in a manner which is contrary to the protection of the private and personal life of that person or contrary to the law. This also includes the situation where the personal data are inaccurate regarding the purpose of their processing. The relevant person may:

(a) ask the controller or processor for an explanation
(b) require the controller or processor to remedy the situation. This can mean in particular blocking, correcting, supplementing or destroying the personal data.

Remedies

In the event of unlawful processing of personal data, the relevant person may claim damages as well as compensation for non-property loss in court.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?

(A) Administrative remedies and other sanctions

Under the Data Protection Act there are a couple of administrative offences which may be committed in connection with the processing and controlling of personal data. If the DPA concludes that an offence was committed, it may impose a fine, the amount of which depends on the type of offence and whether the perpetrator is a business person or natural person. As an example, a breach of a ban on disclosing personal data, collecting data in a manner which does not correspond to the purpose of the data collection, failure to provide the relevant person with mandatory information or failure to notify the DPA would be administrative offences. The maximum fine is CZK 10,000,000 (approx. €400,000). When deciding on the amount of the fine, the seriousness, manner, duration and consequences of the breach of law and the circumstances under which the breach was committed are particularly taken into account. In practice, fines exceeding CZK 500,000 (approx. €20,000) are usually only imposed in exceptional cases (intentional gross breaches of the regulation, number of relevant persons affected by the breach, etc.).

(B) Judicial remedies

In accordance with Article 22 of Directive 95/46/EC (*Remedies*), the relevant person may file for a court action against the controller in order to seek compensation for a breach of data protection regulations.

(C) Criminal law issues

Act No. 40/2009 Coll., Czech Criminal Code, envisages the crime of 'Unauthorised Disposal of Personal Data' which may be committed in the case of:

(a) a breach of data protection regarding personal data collected by public authorities when carrying out their statutory duties or
(b) a breach of the duty of mandatory confidentiality, imposed or acknowledged by the state (e.g. attorneys-at-law, doctors, priests, etc.)

If such crime has been committed, the penalties are imprisonment (usually up to three years, in exceptional cases up to eight years), prohibition on performing certain business activities, fines or other punishments listed in the Czech Criminal Code.

Hungary

1 What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?

Act CXII of 2011 on the Right of Self-Determination in Respect of Information and the Freedom of Information ('Data Protection Act') is based on Directive 95/46/EC and sets the general framework for data protection. To be precise, it defines personal data and data processing, regulates consent rules, data transfer, the obligations of data processors and the rights and remedies of the relevant persons. The Data Protection Act can be found at the following link: www.naih.hu/files/Infotv-_MO.pdf. There are also several laws which contain sector-specific privacy and security requirements.

The Data Protection Act applies to all data processing operations performed in Hungary that involve personal data. The Data Protection Act also applies if a third-country controller engages a data processor in Hungary or if it is using equipment in Hungary, unless such equipment is used solely for the purpose of transit through the EU. Such data controllers must appoint a representative in Hungary. This approach is stricter than Article 4 of Directive 95/46/EC and Opinion 8/2010 on the applicable law of Article 29 of the Data Protection Working Party: Hungarian law applies to data processing carried out in Hungary even if it takes place in the context of the activities of a foreign data controller.

2 What is the data privacy authority (DPA) in your country?

The supervisory authority established in accordance with Article 28 of Directive 95/46/EC is the Hungarian National Authority for Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság* – '*NAIH*'). Its website can be found at www.naih.hu/.

3 Does an internal data privacy officer or similar need to be appointed?

The following data controllers and processors must appoint or engage an internal data privacy officer – who must hold a law degree, a degree in economics or information technology or an equivalent higher education degree – who is to report directly to the head of the organisation:

(a) data controllers or processors processing nationwide jurisdictional, employment and criminal records
(b) financial institutions
(c) electronic communications service providers and public utility services providers.

Otherwise, the appointment of internal data privacy officers is voluntary.

The so-called 'conference of internal data privacy officers' provides for professional liaison between internal data privacy officers and the DPA on a regular basis. The conference intends to ensure the unified application of the law concerning the protection of personal data and the possibility of getting to know information of public interest.

The president of the DPA convenes the conference as necessary, at least once a year, and determines its agenda. The members of the conference can also be the internal data privacy officers of organisations which are not obliged to appoint such officers. To be able to attend the conference, the appointed officer must register in the internal data privacy officers' registry kept by the DPA.

4. Do most companies have internal privacy policies and external privacy notices?
In some cases, preparing such internal privacy policies is mandatory under Hungarian law, e.g. for financial institutions, public utility companies or electronic communications service providers. Nevertheless, it is also common that companies who do not fall under such obligation – especially multinational companies who process cross-border data flows both within and outside their company group – still introduce internal privacy policies and publish privacy notices.

5. What is deemed as 'personal data'?
Like Directive 95/46/EC, the Data Protection Act does not provide an exhaustive list of data which is considered 'personal data', so this must be assessed on a case-by-case basis. Personal data means any information relating a natural person and any reference drawn from such information. Such information will be treated as personal data as long as the data controller / processor has the necessary technology to identify the relevant person.

In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ('sensitive personal data') which means: (a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, and (b) personal data concerning health, addictions, sex life, or criminal record.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?
Personal data may be processed with the prior, voluntary, express and informed consent of the individual or if the processing is allowed by law. In practice, consent can be given verbally, in writing, electronically or by implication. Electronic consent may be acceptable through, e.g., a click by the relevant person on an 'acceptance button' or 'consent box'. Before ticking, the relevant person should also be given the opportunity to read the relevant privacy policy, which gives information on the data processing. Written consent is required only for processing sensitive personal data (unless the data processing is required by law). However, the data controller must always be in the position to prove that consent has been provided properly and lawfully, so proper archiving is advisable. In line with Article 5(3) of Directive 2002/58/EC, data processors may only place cookies (or similar technologies) on users' computers with their prior consent.

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?
On the basis of Article 7 (c) and (f) of Directive 95/46/EC, personal data can be processed even if obtaining the consent proves impossible or involves a disproportionate effort (cost) and if the processing of personal data:
(a) is necessary for compliance with a legal obligation applicable to the data processor or
(b) the processing is necessary for the purpose of legitimate interests of the data processor or third parties and such necessity is proportionate to the restriction of privacy.

In the above cases personal data may also be processed if the relevant person withdraws his/her consent (which can be done at any time under the law). This exception may be applied, for example, in cases where personal data is necessary for a technical operation – e.g. transmitting the personal data of employees to an IT database due to outsourcing – but would require unreasonable administration and effort to collect the consent individually or if only one person does not consent to the data processing, if this can unreasonably delay or prevent the achievement of the desired goal.

On the basis of Article 7 (d) of Directive 95/46/EC, personal data may also be processed without prior consent if the processing is necessary to protect the vital interests of the relevant person or a third party where the relevant person is physically or legally incapable of giving consent, or in order to prevent or avert an imminent danger posing a threat to the lives, physical integrity or property of persons, and to the extent the processing is necessary and for the length of time such reasons persist.

Article 7 of Directive 95/46/EC has not been properly implemented. For example, the Data Protection Act does not allow the processing of personal data without prior consent if it is necessary for the performance of a contract (in line with Article 7 (b) of Directive 95/46/EC). In addition, the requirement set out above ('obtaining the consent proves impossible or involves a disproportionate effort') cannot be derived from Article 7 of Directive 95/46/EC either. The publicly available guidance of the DPA suggests – on the basis of the response of the European Court of Justice in joined cases C-468/10 and C-469/10 – that due to the improper implementation of Directive 95/46/EC, data processors may apply its provisions directly; however, this must be assessed carefully, and always on a case-by-case basis.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?
The transfer of data to a member state of the European Union/the European Economic Area (EEA) is deemed to be as if data was transferred within the territory of Hungary.

Data processors may transfer personal data to data processors that process data in third countries or technical data processors that technically process data in a third country if
(a) it is expressly approved by the relevant person or
(b) the conditions of 'deemed consent' are met (see question No. 7) and an adequate level of protection of personal data is ensured in the third country.

An 'adequate level of protection of personal data' is ensured if (i) it is established by binding legislation of the European Union, or (ii) there is an international agreement between the third country and Hungary containing guarantees for the rights of relevant persons referred to in the Data Protection Act, their rights to remedies, and for the independent supervision and control of data processing operations. Personal data can also be transferred to third countries for the implementation of international treaties and agreements on international legal aid and also for the avoidance of double taxation, even if the 'adequacy' conditions are not met.

The Data Protection Act does not define what 'binding legislation of the European Union' includes. In practice, it refers to whether the European Commission has determined that the third country ensures an adequate level of protection, the Safe Harbour principles are applied, or an 'EU Model Clause' (standard forms of data transfer agreements which are approved by the European Commission) is concluded in respect of the data transfer. In Hungary, EU Model Clauses may not be filed with the DPA. Since 1 January 2012, entering into other individual data transfer agreements or applying Binding Corporate Rules for International Data Transfers (BCRs) are not considered as providing 'adequate protection' anymore. This modification in the legislation was also strongly criticised by both the industry and the DPA, so there is a chance that this unreasonable restriction will change in the future.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?
A group company is regarded as a third party, and, as above, would either (a) need to independently satisfy the legal requirements for processing personal data, or (b) the data privacy consent provided to the 'original' data controller would have to contain consent to the processing / transfer among the group companies, and the relevant companies should enter into a written data transfer agreement as well.

10. When collecting personal data, what information needs to be given, and how?
The Data Protection Act has implemented the requirements listed in Section IV (*Information to be given to the relevant person*) and Section V (*The Relevant person's Right of Access to Data*) of Directive 95/46/EC as follows:
Before the commencement of data processing the relevant person must be given clear and detailed information of all circumstances in relation to the data processing, including:
(a) the voluntary or mandatory nature of the data processing
(b) the list of the personal data processed
(c) the purpose and legal basis for data processing
(d) the identification of the data controller(s) and the data processor(s)
(e) the duration of the data processing
(f) who can access the data
(g) if there is any data transfer to a third country
(h) the rights and remedies of the relevant persons and
(i) if the data processor will not be able to delete the personal data despite the relevant person's request because the data are needed for legitimate purposes.

If it is impossible or would cause unreasonable costs to notify the relevant persons personally, the information may be provided through the publication of the following information:
(a) the fact of data collection
(b) the scope of the persons affected
(c) the purpose of the data collection
(d) the term of data processing
(e) the identity of the data controller(s) who can access the data
(f) if there is any data transfer to a third country
(g) the rights and remedies of the relevant persons and
(h) the registration number (if any) of data processing at the DPA.

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?
The Data Protection Act does not specify the language of the notices and consents in connection with data processing, so the English language would be deemed sufficient; it is not mandatory to translate such documents into the local language. However, if there is any ambiguity, the data controller must prove that the relevant person understood the language of the notice and consent, so bilingual documents are recommended.

12. What are the specific rules where the data controller has appointed a third party to process personal data?
'Technical data processing' (in Hungarian: *'adatfeldolgozás'*) is a specific term used by the Data Protection Act; it cannot be derived from Directive 95/46/EC. It means the technical operations involved in data processing, performed on behalf of and upon the

instructions of a data controller, irrespective of the method and instruments used for such operations and where it takes place. The engagement of a 'technical data processor' (in Hungarian: '*adatfeldolgozó*') requires a written data processing agreement.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?
In line with Article 6 of Directive 95/46/EC, personal data may be processed to the extent and the duration necessary to achieve the purpose of the processing. Any document containing personal data must be destroyed when no further legitimate grounds for keeping such data can be proved; unless the person whose personal data is stored/recorded has authorised the further storage/recording of the data or such authorisation is provided by law.

As regards specific archiving rules, it is advisable to retain data until the relevant period of limitation has expired. A number of circumstances can make it difficult to establish the date on which this period expires, and there are also a couple of rules under the laws which regulate various specific retention obligations in connection with specific documents (e.g. general period of limitation for civil law claims, employment-related documents, safe-keeping of accounting documents and tax returns, employer's certificates concerning social security and workplace accident allowance, declarations on social security entitlement etc.) Any concerns regarding the retention obligation pertaining to a particular document are assessed on a case-by-case basis.

14. Specify below the mandatory technical, organisational or security measures.
As regards the security measures, the Data Protection Act has implemented the provisions of Section VIII of Directive 95/46/EC (*Confidentiality and Security of Processing*). Personal data must be protected against unauthorised access, alteration, transfer, disclosure by transfer or deletion as well as damage and accidental destruction. Data must be protected against becoming inaccessible due to 'changes in the technology applied'. In order to protect data processed in various databases it must be ensured with adequate technical devices that the data stored in databases cannot, unless permitted by law, directly be linked to each other and traced back to the relevant persons. Additional security measures and safeguards are specified for automated personal data processing. The Data Protection Act does not specify any particular way to perform the above general obligations (e.g. to use a specific technique). Data processors must simply choose the data processing alternative that ensures a higher level of protection for personal data, unless this causes disproportionate difficulties.

The Data Protection Act does not provide further details on the technical and organisational measures mentioned above. The DPA's publicly available investigations serve as a guideline for the assessment of the appropriateness of the technical and organisational measures: when reviewing such measures of the data controllers, the DPA particularly checks the procedures regarding the exercise of access rights, the logging of data requests and the registration of data processing. Personal data shall be protected against natural disasters, failures in the technology, human errors (intentional data breach, negligence, omission). Internal registers shall be kept separately. Unlawful entry of personal data shall be prevented, and data transfers and data recordings shall be traceable (logging). In case of any malfunctions, data recovery shall be available and all data accesses and errors shall be documented. Back-up copies shall be kept and security incidents shall be reported for internal analysis.

In line with the amended Directive 2002/58/EC, electronic communications service providers have mandatory data security breach notification obligations.

15. Does a data controller have any other specific obligations?

An internal data transfer registry must be kept for the verification of the legitimacy of data transfers and for providing information to the relevant person. The internal data transfer registry must contain the date, legal basis and addressee of the data transfer, together with the scope of the data transferred and any other data set out in the law requiring the data processing.

16. What are the registration obligations at the DPA?

In accordance with Article 18 of Directive 95/46/EC, data processors must register with the DPA in the Data Protection Registry (in Hungarian: '*Adatvédelmi Nyilvántartás*') prior to carrying out any data processing activities. The registration procedure requires the completion of the DPA's standard online forms. It is currently free of charge, and does not require the submission of additional documents (e.g. data transfer agreements). The data transfer can commence only when the registration is made. The DPA makes the registration within eight days; if it fails to do so, the data processing can commence. Upon registration, the data processor receives a registration number, to be indicated in all data processing operations, such as when data is transferred or disclosed. In the event of any change in the registration data, an application for the registration of changes must be submitted to the DPA within eight days of the effective date of the change.

17. Are there any exemptions from the registration obligation?

No registration is required in the Data Protection Registry in the case of processing:

(a) concerning data of employees, members, kindergarten, students, dormitory services, or customers
(b) carried out in accordance with the internal rules of the church or other religious congregation or organisation
(c) that concerns the personal data of a person undergoing medical treatment, for the purposes of health care and preventive measures or for settling claims for benefits and services in the social insurance system
(d) which involves information concerning the provision of social and other benefits to the relevant person
(e) which involves the personal data of persons implicated in an official regulatory, public prosecution or court proceeding to the extent required for such proceeding, or concerns personal data processed by penal institutions in the execution of a sentence
(f) which involves personal data for official statistical purposes, provided there are adequate guarantees that the data is rendered permanently anonymous in such a way that the relevant person is no longer identifiable in accordance with the relevant legislation
(g) which involves the data of a media content provider, which are used solely for its own information activities
(h) if it serves the purposes of scientific research, and if the data is not made available to the public or
(i) which involves documents deposited in archive.

For the purposes of point (a), the processing of customers' data is exempt from the notification obligation if the data are collected directly from the customers, the customers are adequately informed of the terms of the data processing (including the purpose of the processing, the scope of the data collected and the data retention period), the data are not used for any other purpose and the data are not transferred to third parties without the customer's consent.

18. Are there any specific notification obligations?

Even if certain data processing activities do not require registration, the following data processing activities must be registered with the DPA:

— The DPA's recommendation provides that the transfer of employees' personal data to a third country and/or the operation of whistleblowing systems must be reported to the Data Protection Registry, because such transfers are deemed as 'specific' processing of the personal data of employees.
— Under the Data Protection Act, financial institutions, public utility companies and electronic telecommunications service providers must register with the DPA prior to carrying out any data processing activities in relation to their customers.
— The DPA must register the following data processing operations within 40 days of receiving the application if the data are not affected by the controller's previous data processing operations, or if the controller is using a new processing technique that it has never used before:
  - data files concerning nationwide authorities of jurisdiction, employment and criminal records
  - customer data of financial institutions and public utility companies and
  - customer data of electronic communications service providers.

19. Does the relevant person have the right to access, rectify, remove or block their personal data?

In line with Article 12 (*Right of access*) of Directive 95/46/EC, the relevant person has the following rights:

Information

The relevant person may request confirmation on whether or not data relating to him/her are being processed, including the sources from where they were obtained, the purpose, legal basis and duration of processing, the name and address of the technical data processor and on its activities relating to data processing, and – if the personal data of the relevant person is transferred to third parties – the legal basis and the recipients. The data processor must comply with requests for information without delay, and provide the information requested in an intelligible form within no more than 30 days. This information must be provided free of charge for any category of data once a year. The DPA must be notified of refused information requests for a given year by 31 January of the next year.

Rectification

Data processors must rectify all incorrect personal data.

Deletion

Personal data must be deleted (with the exception of those processed on the basis of law) if:

(a) processed unlawfully
(b) so requested by the relevant person
(c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by law
(d) the purpose of processing no longer exists or the legal time limit for retention has expired
(e) so instructed by court order or by the DPA.

Blocking

Personal data must be blocked instead of deleted if so requested by the relevant person, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the relevant person. Blocked data may be processed only for the purpose which prevented their deletion.

When personal data is rectified, blocked or deleted, the person to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification is not required if it does not violate the rightful interest of the relevant person with a view to the purpose of processing.

Objection

The relevant person has the right to object to the processing of the personal data in the following cases:

(a) if processing or disclosure is carried out solely for the purpose of discharging the controller's legal obligation or for enforcing the rights and legitimate interests of the controller, the recipient or a third party, unless processing is mandatory
(b) if personal data are used or disclosed for the purposes of direct marketing, public opinion polling or scientific research and
(c) in all other cases prescribed by law.

In the event of an objection, the data controller must investigate the cause of the objection within the shortest possible time within a 15-day time period, adopt a decision as to merits and notify the relevant person in writing of its decision.

If, according to the controller's findings, the relevant person's objection is justified, the controller will terminate all processing operations, block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures. These recipients will then take measures regarding the enforcement of the objection.

Appealing to the DPA or to court

The relevant person may also appeal to the DPA or a court in the case of the unlawful processing of his/her personal data.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?

(A) Administrative remedies and other sanctions

If the provisions of the Data Protection Act are violated, the DPA is entitled to the following:

(a) order the rectification of any personal data that is deemed inaccurate
(b) order the blocking, erasure or destruction of personal data processed unlawfully
(c) prohibit the unlawful handling or processing of personal data
(d) prohibit the cross-border transmission or disclosure of personal data
(e) order the provision of an information to the relevant person, if it was refused by the data controller unlawfully
(f) impose a fine of between HUF 100,000 (approx. €370) and HUF 10,000,000 (approx. €37,037) and
(g) publish its resolution, indicating the identification data of the controller as well, where this is deemed necessary for data protection reasons or in connection with the rights of large numbers of relevant persons.

In order to decide whether imposing a fine is justified and to determine the amount of the fine, the DPA will take into account all the circumstances of the case, including the scope of persons affected by the violation of the law, and the gravity or repeated nature of the violation of the law.

(B) Judicial remedies

In accordance with Article 22 of Directive 95/46/EC (*Remedies*), the Data Protection Act enables a relevant person to file for court action against the controller.

(C) Criminal law issues

In serious cases, unlawful data processing may also be deemed as 'Misuse of Personal Data', 'Illicit Access to Data', 'Violation of the Privacy of Correspondence' or 'Invasion of Privacy' under Act C of 2012 on the Hungarian Criminal Code, which may also be punished by imprisonment.

Poland

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?

Directive 95/46/EC has been implemented by the 1997 Act on Personal Data Protection ('Data Protection Act'). It sets the general framework for the protection of personal data in Poland.

The Data Protection Act defines personal data, sensitive data and data processing. It sets rules regarding data transfer, registration, consent rules and the obligations of both data controllers and data processors. It also concerns the rights of data subjects and authorities and relevant remedies.

The Data Protection Act applies to public entities (such as national authorities and local government authorities) as well as to private entities, in particular:

— non-public bodies carrying out public tasks, and
— individuals and legal entities, and organisational units that are not legal entities, if they are involved in processing personal data as a part of their business or professional activity or as part of the pursuit of statutory objectives

seated in Poland or in non-EEA countries, and processing personal data using technical devices located in Poland.

The Act does not apply to:

— individuals involved in data processing exclusively for personal or domestic purposes
— data controllers seated in a non-EEA country whose processing activities are restricted to transferring personal data by means of technical devices located in Poland
— certain journalistic activity that does not violate the rights and freedoms of data subjects.

The Data Protection Act is available at the following link: www.giodo.gov.pl/144/id_art/171/j/en/.

More specific regulations concerning data processing in Poland are:

— the 2004 Regulation concerning the template for notifying the General Inspector for Personal Data Protection of a database
— the 2004 Regulation concerning documentation for processing personal data, and technical and organisational requirements for devices and computer systems used for processing personal data.

Additional regulations on personal data protection can be found in acts relating to particular areas of business or business practice, for example:

— the Insurance Activity Act 2003
— the Banking Law Act 1997
— the Labour Code Act 1974.

2. What is the data privacy authority (DPA) in your country?
The supervisory authority established in accordance with Article 28 of Directive 95/46/EC is the Polish General Inspector for Personal Data Protection (GIODO) (*Generalny Inspektor Ochrony Danych Osobowych* – '*GIODO*'). Its website can be found at www.giodo.gov.pl/168/j/en.

3. Does an internal data privacy officer or similar need to be appointed?
A data controller must appoint an administrator of information security who supervises compliance with security principles provided by the law. If the data controller performs supervision activities itself, an administrator of information security does not have to be appointed.

4. Do most companies have internal privacy policies and external privacy notices?
Internal privacy policy
Under Polish law, there is no obligation to keep an internal privacy policy document. However, data controllers are obliged to implement technical and organisational security measures to protect processed data, depending on the dangers and categories of data. These measures have to be described in the documentation maintained by the data controller. This means that each data controller and data processor (if data processing has been entrusted to another company) must keep the following internal documentation: Security Policy and Instructions on Managing Computing Systems Used for Personal Data Processing. As regards the contents of such documents, please see section 14 below.

External privacy notice
There is no obligation to have an external privacy notice. However, if a company provides on-line services, external terms and conditions of the service should be available on the company's website. The terms and conditions must state the type and scope of on-line services, the technical requirements, the conditions of concluding contracts, and the complaints procedure. The customer should be able to download these regulations in order to record and review them in a reproducible form. Customers should also receive (directly through the system) clear and unambiguous information on: electronic addresses of the on-line service provider and its name and address, particular threats related to the use of such services, functionality of the software used by the on-line service provider and the possibility of discontinuing the services at any time.

5. What is deemed as 'personal data'?
Like Directive 95/46/EC, the Data Protection Act does not provide an exhaustive list of the data which is deemed as 'personal data'. 'Personal data' is defined as data relating to an identified individual, or relating to an individual who can be identified from such data (the data subject).

In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ('sensitive personal data') which means: (a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, political party or trade-union membership, and (b) personal data concerning health, genetic code, addictions and sexual orientation, or criminal record and (c) personal data relating to criminal convictions, decisions on penalties, fines and other decisions issued in court or administrative proceedings.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?

In most cases, the data subject's prior, voluntary, express and informed consent is required before personal data can be processed. Consent of the data subject is the most common legal basis for processing data. No specific form of the data subject's consent is required.

In practice, consent can be given verbally, in writing or electronically. Electronic consent may be acceptable through – for example – a click by the relevant person on an 'acceptance button' or 'consent box'.

Processing of sensitive data as well as the transfer of data outside the European Economic Area requires written consent (but there are some exceptions).

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?
A data controller may process personal data without the consent of the data subject when the data processing:
— involves only erasing personal data
— is essential for the purpose of exercising rights or duties resulting from a legal provision
— is necessary for the performance of an agreement to which the data subject is a party, or is necessary to take certain steps, at the data subject's request, prior to entering into an agreement
— is necessary for the performance of certain tasks provided for by law and carried out in the public interest
— is necessary for the purpose of legitimate interests pursued by the data controllers or data recipients, provided that it does not violate the rights and freedoms of the data subject
— is necessary to protect the vital interests of the data subject, and consent cannot be obtained (this exemption applies only until such time when consent may be obtained).

There are some exceptions that allow for the processing of sensitive personal data without the data subject's consent. These exceptions include situations where:
— the data processing involves only erasing sensitive personal data
— the specific provisions of another act provide for processing such sensitive personal data without the data subject's consent, and provide for adequate safeguards
— the data processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically/legally incapable of giving his/her consent until a guardian/curator can be established
— the data processing is necessary to pursue a legal claim
— the data processing is necessary to enable the data controller to perform its obligations with regard to the employment of its employees and other individuals, and is permitted by employment law
— the data processing is required in certain medical contexts
— the data processing relates to sensitive personal data that has been made publicly available by the data subject
— the data processing is conducted to exercise rights and duties resulting from decisions issued in court or administrative proceedings.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?
The legal requirements for transferring personal data to another country depend on the country of destination. There are different requirements related to transferring data between entities with their seats in the European Economic Area (EEA) and to those outside it. In short, transferring personal data within the EEA does not require taking any additional steps other than executing a data transfer agreement and, in some cases notifying the GIODO.

Data may only be transferred outside the EEA if the laws of the country of destination ensure at least the same level of data protection as Polish law.

This requirement does not apply in certain circumstances including those where:
— the transfer is required by law or by the provisions of 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 in the interests of the data subject between the data controller and another person
— the transfer is necessary for reasons of public interest or for legal claims
— the transfer is necessary in order to protect the vital interests of the data subject
— the transfer relates to personal data that is publicly available.

For transfers to non-EEA countries where the data protection laws fall below the required standard and if any of the above prerequisites has not been fulfilled, prior consent must be obtained from the GIODO. The data transfer can then only take place when the GIODO has granted consent. In general, the consent should be issued without undue delay, but it may take up to eight months.

Personal data can be transferred to non-EEA countries with lower data protection standards if the GIODO's consent has been issued and provided that the data controller ensures adequate safeguards with respect to the protection of the privacy, rights and freedoms of the data subject. Adequate safeguards means protection in accordance with the Polish regulations relating to the safety of personal data. Such safeguards are measured on a case-by-case basis. Implementation of EC Model Clauses or Binding Corporate Rules does not allow for the free transfer of data from Poland to third countries without the GIODO's consent. Certification under the Safe Harbour programme is sufficient ground for the transfer of data to the certified entity.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?

Other group companies are regarded as being third parties, and, as above, would either need to independently satisfy the legal requirements for processing personal data, or could enter into a data controller – data processor agreement. Group companies must fulfil the same requirements (e.g. technical and organisational measures implemented to protect processed data) as an external company that processes personal data.

10. When collecting personal data, what information needs to be given, and how?

The Data Protection Act has implemented the requirements listed in Section IV (*Information to be given to the relevant person*) and Section V (*The Relevant person's Right of Access to Data*) of Directive 95/46/EC as follows:
When collecting data, the data controller is obliged to inform data subjects of the following:

(a) the address of its seat and its full name, and if the controller is a natural person – its name and surname and address
(b) the purpose of data collection, and, in particular, about the data recipients or categories of recipients, if known on the date of collecting
(c) whether the consent to the data processing is obligatory or voluntary, and in the case of the existence of the obligation about its legal basis
(d) the right of the data subject to access his/her data and to rectify the data.

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?

The Data Protection Act does not specify the language of notices and consents in connection with data processing, so the English language would be deemed sufficient. It is not mandatory to translate such documents to the local language. However, in the case of any ambiguity, the data controller must prove that the relevant person has understood the notices and consents, so bilingual documents are recommended.

12. What are the specific rules where the data controller has appointed a third party to process personal data?

A data controller may outsource personal data processing to third parties. Companies from the same capital group as the data controller may be deemed as third parties. A company that processes personal data on behalf of the data controller (for purposes determined by the data controller) is treated as a data processor.

The engagement of a data processor requires a written data processing agreement. The data processor may process data solely within the scope and for the purpose determined in the agreement. Prior to processing, the data processor is obliged to implement the same security measures as provided for at the data controller.

The GIODO must be notified about the entrustment of data processing.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?

In general, in line with Article 6 of Directive 95/46/EC, personal data may be processed to the extent and the duration necessary to achieve the purpose of the processing.

Any document containing personal data must be destroyed when no further legitimate grounds for keeping such data can be proved, unless the person whose personal data is stored/recorded has authorised the further storage/recording of the data or such authorisation is provided by law.

As regards specific archiving rules, it is advisable to retain data until the relevant period of limitation has expired. A number of circumstances can make it difficult to establish the date this period expires, and there are also some rules that arise under the laws which regulate specific retention obligations for specific documents (e.g. general period of limitation for civil law claims, employment related documents, safe-keeping of accounting documents and tax returns, employer's certificates concerning social security and workplace accident allowance, declarations on social security entitlement etc.) Any concerns regarding the retention obligation for a particular document are assessed on a case-by-case basis.

14. Specify below the mandatory technical, organisational or security measures.

Mandatory security measures

In Poland the rules for technical and organisational measures in relation to computerised processing of personal data are stricter than those under EU legislation. It is important for the GIODO that IT systems used for processing personal data meet the technical requirements provided by the law.

Processing personal data in a computer system requires the appropriate security level. The security level depends on the category of data processed (non-sensitive personal data or sensitive personal data) and the risk of a data leak. The security levels are as follows: basic security level, medium security level and high security level. Each security level has particular requirements as regards measures that should be implemented, described in detail in the 2004 Regulation concerning documentation for processing personal data, as well as technical and organisational requirements for devices and computer systems used for processing personal data.

Security measures required by the law in relation to the appropriate security level:

Basic security level
Basic security level applies if the data controller (or data processor) does not process any sensitive data and none of the computer devices used for processing is connected to the public network.

In this case, the data controller (or data processor) is required to:
— secure the area where data are processed against unauthorised access
— apply an access control mechanism, e.g. magnetic cards
— grant separate identifiers, if at least two users have access to the computer system
— use software that protects data against unauthorised access
— secure data against loss caused by power failure
— secure access to the computer system by a password consisting of at least six characters, and change the password at least once a month
— make back-ups of the databases
— if data are processed on mobile media devices (laptops, tablets) – take special precautions in transport.

Medium security level
If the data controller (or data processor) processes sensitive data and none of the computer devices used for processing is connected to the public network, all the security measures under the basic level must be applied, but the password used for the user authentication has to consist of at least eight characters, including small and capital letters, numbers and special characters.

High security level
Processing personal data using devices connected to the public network requires high-level security. At this level, the basic- and medium-level security measures must be applied, and additionally the computer system must be secured against any dangers from the public network. The data controller (or data processor) must implement physical and logical security measures that protect the system from any unauthorised access.

Mandatory documentation describing implemented security measures
A data controller (and data processor) is obliged to keep a Security Policy, i.e. documentation on the protection of processed personal data. The Security Policy describes the factual scenario of processing personal data, as well as the security measures used and internal policies related to data protection.

The data controller (and data processor) is also required to produce Instructions on Managing Computing Systems Used for Personal Data Processing. This document should describe the procedure of granting authorisation or access to processed data in the data processing system. The Instructions must also include descriptions of the following: the means of authenticating computer users, procedures of launching, completing and suspending work on computing systems, information on back-ups, storage of data carriers, a description of security means against malicious software, information on whether the system automatically registers when and by whom the data are entered into the computing system, and to whom the data are revealed, and procedures of maintenance of computing systems and media carriers.

15. Does a data controller have any other specific obligations?
Besides the obligation to hold a valid legal basis for processing data, to implement technical and organisational security measures to protect processed data, to inform data subjects about processing their data, to submit a motion to the GIODO to register a database and to obtain a legal basis for transfers outside the EEA, a data controller and data processor are obliged to monitor who has access to the processed data by authorising selected persons and keeping a register of them and to ensure supervision over which data, when and by whom have been entered into the database and to whom they are transferred.

16. What are the registration obligations at the DPA?
A data controller is obliged to notify the GIODO about any database and to submit it for registration. A database includes any structured set of personal data. The personal data in a database can be processed after the database has been submitted for registration, unless it contains sensitive personal data. Processing sensitive data requires GIODO's registration of the database. There is no statutory term for the GIODO to issue a decision on denial of registration of a database (the GIODO only issues decisions on denial and not on registration).

The notification must be submitted on a special form in hard copy, as specified in the 2004 Regulation on the template for GIODO notifications or on-line through the on-line registration service provided by the GIODO at the following address: egiodo.giodo.gov.pl/formular_step0.dhtml?c=0.6361029927790196.

The notification itself should not include the content of the actual data, but should specify the following:
(a) that it is an application to enter the database into the GIODO's register of databases
(b) details concerning the entity running the database, and the legal grounds on which that person is authorised to run the database
(c) the purpose of the processing of the personal data
(d) a description of the categories of data subjects and the scope of the processed data
(e) information on the methods of data collection and disclosure – information on the recipients or categories of recipients to whom the data may be transferred
(f) a description of the technical and organisational security measures
(g) information relating to any possible data transfer to a non-EEA country.

17. Are there any exemptions from the registration obligation?
The data controller is not obliged to notify the GIODO in certain cases, including those where the personal data:
— is a state secret
— has been collected as a result of certain official inquiry procedures
— is processed in connection with the data controller's employment of (or similar service agreements with) the data subjects
— refers to individuals using healthcare, legal, notary, patent agency, tax consultancy or auditor services
— is processed for the purpose of issuing an invoice, bill or for accounting purposes
— is publicly available
— is processed with regard to minor current everyday affairs.

18. Are there any specific notification obligations?
The data controller is obliged to notify the GIODO of any change of the following information:
— name and address of the data controller and the legal grounds for processing the data
— name and address of the data processor / processors
— the categories and scope of the processed data
— recipients or categories of recipients of the data
— technical and organisational measures used for the security of the processed data
— transfer of data to third countries.

The GIODO should be notified of any change to the above information within 30 days of the change being introduced into the database.

19. Does the relevant person have the right to access, rectify, remove or block their personal data?

In line with Article 12 (*Right of access*) of Directive 95/46/EC, the relevant person has the following rights:

Information

The relevant person may request extensive information on whether a database exists, and the data controller's identity, the address of its seat and its full name. If the data controller is a natural person, the relevant person may obtain the following: the data controller's full name and address, information on the purpose, scope, and means of processing the data contained in the system, information on when his/her personal data were first processed and information in an intelligible form on the content of the data, information on the source of the personal data, unless the data controller is obliged to keep it confidential as a state, trade or professional secret, information about the means in which the data are disclosed, and in particular about the recipients or categories of recipients of the data.

Modification, rectification, suspension and erasure

Data subjects may demand their data to be completed, updated, rectified, temporarily or permanently suspended or erased, in case the data are incomplete, outdated, untrue or collected in violation of the data protection law, or if the data are no longer required for the purpose for which they were collected.

Blocking

The relevant person can make a justified demand in writing for blocking the processing of his/her data, due to his/her particular situation, when the data are processed on the grounds of tasks for the public good or when processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients.

Objection

The relevant person has the right to object to the processing of his/her personal data (processed on the grounds of tasks for the public good or the purpose of legitimate interests) if the data controller intends to process data for marketing purposes. The relevant person may also object to the transfer of the data to another controller.

Appealing to the GIODO

The relevant person may also appeal to the GIODO in the case of the unlawful processing of his/her personal data.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?

(A) Administrative remedies and other sanctions

If the data controller violates the Polish data protection provisions, the GIODO may issue an administrative decision and oblige the data controller to:

(a) remedy the negligence
(b) complete, update, correct, disclose or not disclose personal data
(c) apply additional measures to protect the processed data
(d) suspend data flow to a third country (and thus suspend a project)
(e) erase the personal data.

If the data controller does not implement the GIODO's decision, the GIODO may impose a fine in order to compel enforcement of the decision in the amount of up to PLN 200,000 (approximately US $60,000) for companies and up to PLN 50,000 (approximately US $15,000) for individuals.

(B) Judicial remedies

In accordance with Article 22 of Directive 95/46/EC (*Remedies*), the relevant person may file for a court action against a data controller in the case of a violation or threat of a violation of his/her personal rights.

(C) Criminal sanctions

Disclosure of personal data or providing access to unauthorised persons may lead to a fine, limitation of liberty or deprivation of liberty for up two years. If the data are sensitive, imprisonment may be up to three years.

If a data controller does not provide appropriate security measures to protect data against unauthorised takeover, damage or destruction, the person responsible for such protection will be liable to a fine, restriction of liberty or deprivation of liberty for up to one year.

Failure to notify the GIODO of a database for registration or interrupting the GIODO's inspection may also result in criminal liability.

Romania

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?
Act no. 677 regarding the protection of individuals with regard to processing their personal data and the free movement of such data of 2001 ('Data Protection Act') is based on Directive 95/46/EC and sets the general framework for data protection. To be more precise, it defines personal data and data processing, regulates consent rules, data transfer, the obligations of data processors and the rights and remedies of the relevant persons. The Data Protection Act can be found at the following link: www.dataprotection.ro/index.jsp?page=legislatie_primara&lang=en.

There are also several laws which contain sector-specific privacy and security requirements.

The Data Protection Act applies to all data processing operations performed in the territory of Romania that pertain to the data of natural persons. The Data Protection Act also applies if a third-country controller engages a data processor situated in Romania or if it is using equipment in Romania, unless such equipment is used solely for the purpose of transit through the EU. Such data controllers must appoint a representative in Romania.

2. What is the data privacy authority (DPA) in your country?
In accordance with Article 28 of Directive 95/46/EC, the National Supervisory Authority for Personal Data Processing (Autoritatea Nationala de Supraveghere a Prelucrarilor de Date cu Caracter Personal – 'ANSPDCP') was established. Its website can be found at www.dataprotection.ro/.

3. Does an internal data privacy officer or similar need to be appointed?
The appointment of internal data privacy officers is voluntary, meaning that under the Data Protection Act there is no obligation on controllers to designate an internal data privacy officer.

4. Do most companies have internal privacy policies and external privacy notices?
Under the Data Protection Act, companies that process individuals' personal data have an obligation to introduce internal privacy policies and publish privacy notices on the processing of such individuals' personal data.

The Data Protection Act does not expressly regulate the content of such internal privacy policies and external privacy notices. Normally, such policies address issues related to the purposes of processing, the categories of personal data that are processed, processing measures etc. As companies are obliged to observe certain minimum security measures when processing personal data (e.g. supervised access to the personal data, identification and

log-on requirements for employees within the company who process personal data etc.), there is usually a description of these minimum security measures in the internal privacy policies.

Moreover, pursuant to the secondary data protection legislation (namely Order no. 52/2001 approving the minimum technical security measures, issued by the Romanian Ombudsman), there are some minimum security measures that must be implemented by the data controller when it processes personal data. In practice this usually involves including a description of such minimum security measures in the data privacy policy, among other things.

5. What is deemed as 'personal data'?
Like Directive 95/46/EC, the Data Protection Act does not provide for an exhaustive list of data which is deemed 'personal data', so it should be assessed on a case-by-case basis. Personal data means any information relating to a natural person and any reference drawn from such information. Such information should be treated as personal data when a data controller / processor has the necessary technology to identify the relevant person.

In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ('sensitive personal data') which means: (a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, and (b) personal data concerning health, addictions, sex life, or criminal record.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?
Personal data may be processed only with the relevant person's prior, voluntary, express and informed consent, with the exception of cases when the processing is allowed by law. In practice such consent can be given in writing or electronically. Electronic consent may be acceptable through – for example – a click by the relevant person on an 'acceptance button' or 'consent box'. Before clicking, the relevant person should be given an opportunity to read the privacy policy, which sets out the information on the data processing. Written consent only is required for processing sensitive personal data (unless the data processing is required by law). However, the data controller must always be in a position to prove that the consent was provided properly and lawfully, so proper archiving is advisable. In line with Article 5(3) of Directive 2002/58/EC, data controllers / processors may only place cookies (or similar technologies) on users' computers with their prior consent.

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?
Article 7 of Directive 95/46/EC was entirely implemented under the Data Protection Act. As a result, all exceptions provided under letters b) to f) of Article 7 on processing personal data without the relevant person's consent would apply as per Article 5 of the Data Protection Act.

In addition, under Article 5 of the Data Protection Act, processing personal data can be performed without the relevant person's consent if such processing is performed for statistical, historical or scientific purposes, provided that the data remains anonymous (as per Article 11.2 of Directive 95/46/EC), or if processing is related to data resulting from publicly available documents.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?
The transfer of data to a European Union/European Economic Area member state is deemed to be as if data was transferred within the territory of Romania. Such transfer requires the controller/ processor to submit a prior notification to the DPA.

Data controllers may transfer personal data to recipients located in countries outside the European Union/the European Economic Area (i.e. data controllers or processors that process data in third countries or technical data processors that technically process data in a third country) if
(a) the transfer is expressly approved by the relevant persons whose data will be transferred or
(b) the transfer is performed under Romanian law, and an adequate level of protection of personal data is ensured in the third country.

The DPA assesses 'adequate level of protection of personal data' on a case-by-case basis, by taking into consideration, *inter alia*, the nature of the data to be transferred, the processing scope and the proposed duration of the processing. The DPA's assessment of an 'adequate level of protection of personal data' will not be necessary if (i) protection is established by sector-specific legislation, or (ii) there is an international agreement between the third country and Romania containing guarantees of the rights of the relevant persons referred to in the Data Protection Act, their rights to remedies, and of the independent supervision and control of data processing operations. Personal data can also be transferred to third countries for the implementation of international treaties and agreements on international legal aid as well as for the avoidance of double taxation, even if the 'adequacy' conditions are not met. The DPA must have prior notification of the transfer.

If the transfer of personal data is to be made to recipients located in third countries where an 'adequate level of protection of personal data' is not ensured, the DPA must have prior notification of the transfer and give its authorisation. The DPA's authorisation will be given based on guarantees granted by the data controller, and relating to the protection of the fundamental rights of individuals. Such guarantees have to be included in the processing agreement concluded with the recipient. For this purpose, the DPA transposed into national law the Standard Clauses for Data Processors established in Third Countries, as adopted by the European Commission. Such standard clauses must be in the Romanian language.

The DPA did not adopt specific BCR local legislation. However, in practice, the recommendations of the 29 Article Working Party apply.

In the case of U.S. recipients which have implemented the Safe Harbour principles, no prior authorisation will be needed. However, in practice, the DPA may require the data controller to provide proof that the personal data recipient holds Safe Harbour certification.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?

A group company is regarded as a third party, and, as above, would either (a) need to independently satisfy the legal requirements for processing personal data, or (b) the data privacy consent provided to the 'original' data controller would have to contain consent to the processing/transfer among the group companies and the relevant companies should enter into a written data transfer agreement as well.

10. When collecting personal data, what information needs to be given, and how?

The Data Protection Act has implemented the requirements listed in Section IV (*Information to be given to the relevant person*) and Section V (*The Relevant person's Right of Access to Data*) of Chapter II of Directive 95/46/EC.

In relation to data processing, the relevant person whose data will be processed must be given clear and detailed information of all circumstances, including:

(a) the voluntary or mandatory nature of the data processing
(b) a list of the personal data processed
(c) the purpose and legal basis of data processing
(d) who the data controller(s) and the data processor(s) are
(e) the duration of the processing of the data
(f) who has access to the data
(g) if any data are transferred to a third country
(h) the rights and remedies of the relevant persons and
(i) if the data processor is not able to delete the personal data despite the relevant person's request because the data are needed for legitimate purposes.

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?

The Data Protection Act does not specify the language of the notices and consents in connection with data processing, but as under art. 13 of Romanian Constitution the official language is Romanian, Romanian language is expected in relation to notice and consent.

12. What are the specific rules where the data controller has appointed a third party to process personal data?

Under the Data Protection Act an 'authorised person' (Rom. "persoană împuternicită") is a third party appointed by the data controller to process personal data on the data controller's behalf. The term is used by Directive 95/46/EC. The engagement of an 'authorised person' requires a written data processing agreement that must outline the fact that proper guarantees are in place in order for the authorised person to protect the personal data that it processes on behalf of the data controller against damage resulting from, among other things, destruction, loss, amendment or disclosure.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?

In line with Article 6 of Directive 95/46/EC, personal data may be processed to the extent and the duration necessary to achieve the purpose of the processing. Any document containing personal data must be destroyed when there are no further legitimate grounds to keep the data, unless the person whose personal data is stored/recorded has authorised the further storage/recording of such data or such authorisation is provided by law.

As regards specific archiving rules, it is advisable to retain data until the relevant period of limitation has expired. A number of circumstances can make it difficult to establish the date on which this period expires and there are a couple of rules arising under the laws which regulate various specific retention obligations in connection with specific documents (e.g. general period of limitation for civil law claims, employment-related documents, safe-keeping of accounting documents and tax returns, employer's certificates concerning social security and workplace accident allowance, declaration on social security entitlement etc.) Any concerns regarding the retention obligation pertaining to a particular document are assessed on a case-by-case basis.

14. Specify below the mandatory technical, organisational or security measures.

As regards the security measures, the Data Protection Act has implemented the provisions of Section VIII of Chapter II of Directive 95/46/EC (*Confidentiality and Security of Processing*). Personal data must be protected against unauthorised access, alteration, transfer, disclosure by transfer or deletion as well as damage and accidental

destruction. Data must be protected against becoming inaccessible due to 'changes in the technology applied'. In order to protect data processed in various databases it must be ensured with adequate technical devices that the data stored in databases cannot, unless permitted by law, be directly linked to other data and traced back to the relevant persons. Additional security measures and safeguards are specified for automated personal data processing. The Data Protection Act does not specify any way to perform the above general obligations (e.g. to use a specific technique). Furthermore, pursuant to Order no. 52/2002 *on minimum security technical measures* as issued by the Ombudsman, certain minimum security measures must be implemented by each data controller.

In line with the amended Directive 2002/58/EC, electronic communications service providers have mandatory data security breach notification obligations.

15. Does a data controller have any other specific obligations?

In all cases, the DPA must be notified of any transfer of data outside Romania, for the verification of the legitimacy of the data transferred and for assessing the adequacy of the level of protection in the country where such data is to be transferred. In order to lawfully commence the data transfer, it is necessary to wait for the DPA's feedback. Usually, the DPA provides its feedback (i.e. will allow or refuse the transfer) within a maximum period of 30 calendar days as of the submission of the complete notification with the DPA.

16. What are the registration obligations at the DPA?

In accordance with Article 18 of Directive 95/46/EC, data processors must notify the DPA, prior to carrying out any data processing activities. The registration procedure requires the completion of the standard online forms of the DPA and it is currently free of charge.

Upon registration, the data processor receives a registration number, to be indicated in all data processing operations, such as when data is transferred or disclosed. In the event of any change in the registration data, an application for the registration of changes must be submitted to the DPA within five days from the effective date of the change.

The data processor notification and registration number is registered with the Data Protection Registry, and is publicly available for inspection at the following address: www.dataprotection.ro/notificare/cautari.do

17. Are there any exemptions from the registration obligation?

No registration is required in the Data Protection Registry in case of the processing of personal data related to:

(a) keeping a registry designed for public information
(b) claims submitted by petitioners to public authorities, that are to be reviewed as part of such authorities' legal obligations
(c) employees and external collaborators, to comply with a legal obligation
(d) owners or tenants, by owners or tenants associations
(e) the economic-financial, public relations or administrative activity of public or private companies
(f) individuals who participate in a contest or exam for hiring purposes, or who submit their resumes in this regard
(g) individuals participating in conferences or exams
(h) members of associations or NGOs for the purpose of performing their activities, without disclosure to third parties
(i) clergy activities
(j) individuals whose files are in the archive of the National Council for the Study of Securitate Archives, if such processing is limited to either journalistic, literary, artistic, statistical, historical or scientific research or to review their own files
(k) journalistic, literary or artistic purposes

(l) individuals performing an independent activity (such as lawyers)
(m) use of the National Archives database, or use by libraries
(n) activities of courts of law
(o) real estate activities
(p) members of political parties, provided that such data is not disclosed to third parties.

18. Are there any specific notification obligations?
The processing of certain activities requires notification to the DPA, e.g.:
— if the personal data to be processed falls under the category of 'special data', as listed under Article 8.1 of Directive 95/46/EC, or is related to an individual's genetic, biometric or geographical location
— if the personal data to be processed relates to criminal or administrative sanctions of various individuals
— if the personal data to be processed relates to an assessment of an individual's personality, such as professional competence, credibility, behaviour, or to a decision made by automatic individual means
— if the personal data to be processed relates to minors.

19. Does the relevant person have the right to access, rectify, remove or block their personal data?
In line with Article 12 (*Right of access*) of Directive 95/46/EC, the relevant person has the following rights:

Information
The relevant person may request confirmation as to whether or not data relating to him/her are being processed, including the sources from where they were obtained, the purpose, legal basis and duration of processing, the name and address of the technical data processor and information on its activities relating to data processing, and - if the personal data of the relevant person is transferred to third parties - the legal basis and the recipients. The data processor must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days. The information specified above must be provided free of charge for any category of data at least once a year.

Rectification
Data processors must rectify any incorrect personal data.

Deletion
Personal data must be deleted (with the exception of data processed on the basis of law) if:
(a) it is processed unlawfully
(b) the relevant person makes such a request
(c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by law
(d) the purpose of processing no longer exists or the legal time limit for retention has expired
(e) it is instructed to do so by a court order or by the DPA.

Blocking
Personal data will be blocked instead of deleted if so requested by the relevant person, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the relevant person. Blocked data may be processed only for the purpose which prevented their deletion.

If personal data is rectified, blocked or deleted, the relevant person to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification is not required if it does not violate the rightful interest of the relevant person with a view to the purpose of processing.

Objection

The relevant person has the right to object to the processing of the personal data:

(a) if the processing or disclosure is carried out solely for the purpose of discharging the controller's legal obligation or for enforcing the rights and legitimate interests of the controller, the recipient or a third party, unless processing is mandatory
(b) if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research and
(c) in all other cases prescribed by law.

In the event of an objection, the data controller must investigate the cause of the objection within the shortest possible time within 15 days, adopt a decision as to the merits and notify the relevant person in writing of its decision.

If, according to the findings of the controller, the relevant person's objection is justified, the controller must terminate all processing operations, block the data in question and notify all recipients to whom any of these data had previously been transferred about the objection and the ensuing measures. These recipients should then also take measures regarding the enforcement of the objection.

Appealing to the DPA or to the court

The relevant person may also appeal to the DPA or a court in case of the unlawful processing of his/her personal data.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?

(A) Administrative remedies and other sanctions

In the case of a violation of the provisions of the Data Protection Act, the DPA is entitled to the following:

(a) order the rectification of any personal data that is deemed inaccurate,
(b) order the blocking, erasure or destruction of personal data processed unlawfully,
(c) prohibit the unlawful handling or processing of personal data,
(d) prohibit the cross-border transmission or disclosure of personal data,
(e) order access to the relevant person's information, if it was refused by the data controller unlawfully,
(f) impose a fine of between RON 500 (approx. €111) and RON 50,000 (approx. €11,111).

In order to decide whether imposing a fine is justified and to determine the amount of the fine, the DPA will take into account all the circumstances of the case, including the scope of persons affected by the violation of the law, and the gravity or repeated nature of the violation of the law.

(B) Judicial remedies

Under Article 22 of Directive 95/46/EC (*Remedies*), the Data Protection Act enables a relevant person to file for a court action against a data controller.

(C) Criminal law issues

Unlawful personal data processing is not punished by imprisonment or by penal fine under the Romanian Criminal Code.

Russia

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?
Federal Law No. 152 – FZ 'On personal data' dated 27 July 2006, revised and effective since 27 July 2011 ('Data Protection Act') is based on the Strasbourg Convention of 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Strasbourg Convention') and sets a general framework for data protection. To be more precise, it defines personal data and data processing, regulates consent rules, cross-border data transfer, the obligations of data controllers and the rights of natural persons. There are also several legal acts which contain some sector-specific privacy and security requirements (for example, the Labour Code contains some provisions on personal data of employees).

The Data Protection Act applies to all data processing operations performed in the territory of Russia that pertain to the data of natural persons. In particular, the Data Protection Act applies when data processing is performed by Russian state bodies, municipal organs, legal entities and individuals, irrespective of whether they use any automatic measures in this regard.

2. What is the data privacy authority (DPA) in your country?
Control over compliance in the field of personal data protection is performed by the Russian Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (DPA). Its website can be found at www.pd.rsoc.ru/.

3. Does an internal data privacy officer or similar need to be appointed?
The DPA provides that all legal entities that deal with personal data should appoint a person responsible for the organisation and compliance of personal data processing. However, no specific requirements are provided by the DPA with regard to the specific qualifications needed by such a person.

4. Do most companies have internal privacy policies and external privacy notices?
Under the Data Protection Act, personal data controllers are obliged to produce regulations on personal data processing and make them accessible to the public (e.g. publish it on a web-site). The regulations should determine the procedures for avoiding violations of legislative provisions and the measures aimed at eliminating the negative consequences of violations of law.

5. What is deemed as 'personal data'?
Like the Strasbourg Convention, the Data Protection Act does not provide for an exhaustive list of data which is deemed as 'personal data', so it is assessed on a case-by-case basis. Personal data is defined as any information that refers directly or indirectly to an identified or identifiable natural person.

In line with Article 6 of the Strasbourg Convention, the Data Protection Act sets out a special category of data ('sensitive personal data') which means information referring to racial or ethnic origin, information on political opinions, religious or philosophical beliefs, information on state of health, sex life, and criminal record.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?
Personal data may be processed with the prior, voluntary, express and informed consent of the relevant person, or if processing without consent is expressly allowed by law.

Under the Data Protection Act, consent can be given in any form which allows confirmation of the fact that consent was given. In practice it may take the form of consent given verbally, in writing, electronically or by implication. It is necessary, however, that, the data controller is always in a position to prove (in the case of any ambiguity) that consent has been provided properly and lawfully. That is why obtaining consent in an electronic form or verbally remains somewhat risky from the point of view of proving that the consent was obtained. The DPA has not yet formalised its position with regard to such forms of consent.

Under the Data Protection Act, consent should be obtained in the form of a written document (so-called 'qualified consent'), in particular, in the following cases:
a) processing of sensitive personal data
b) cross-border transfer of personal data to states which do not ensure an adequate level of personal data protection.

'Qualified consent' should be established in writing and also contain the following elements:
— name, address and passport details of the relevant person (and a representative of the relevant person, if the data is provided by the representative)
— name and address of the personal data controller
— purposes for processing the personal data
— list of the personal data to be processed for which the consent is given
— name and address of the technical processor which processes the personal data at the request of a personal data controller (if applicable)
— list of operations that will be performed with the personal data, general description of methods that will be used for personal data processing
— the period of time during which the personal data will be processed, and how consent to processing may be withdrawn
— signature of the relevant person (either authentic or electronic).

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?
The Data Protection Act provides a list of 10 exceptions under which personal data may be processed without obtaining the consent of the relevant person.

First of all, the controller is exempt from the obligation to obtain consent from the relevant person, if the personal data is processed for purposes provided by an international treaty signed by the Russian Federation, or by Russian law for the execution of justice, and execution of an act of court.

The same refers to cases where processing personal data is necessary for the protection of the life, health or other vital interests of the relevant person (if it is impossible to obtain his/her consent) or for protecting legal interests and socially important purposes, under the condition that the rights of the relevant person are not violated.

The relevant person's consent is also not required for processing his/her data for the purposes of providing state and municipal services in compliance to the respective legal acts (for example, if a relevant person discloses his/her personal data on the specific state web portal dedicated for providing state services).

This exception also applies to situations where personal data is required for the execution and/or signature of a contract to which the relevant person is a party, beneficiary or guarantor. For example, if a company or an individual enters into an insurance agreement under which the relevant person is a beneficiary, it might not be necessary to obtain the relevant person's consent for processing his/her personal data.

Another situation when it is not necessary to obtain the relevant person's consent is when the rights and legal interests of the controller and third parties need to be protected or in order to achieve socially important purposes (under the condition that the relevant person's rights are not violated).

Journalists performing their professional obligations or other legal activity for the mass media, as well as writers and scientists working within their creative activities, may use personal data without the relevant person's consent, on the condition that the rights of the relevant person are not violated.

Processing personal data which was made public upon the request of the relevant person as well as disclosure of personal data in accordance with the requirements of the law may also be performed without the consent of the relevant person.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?
The transfer of data to a state which ensures an 'adequate level of protection of personal data' (an 'adequate state') is deemed to be as if data was transferred within the territory of the Russian Federation.

A state is considered to ensure an 'adequate level of protection of personal data' if (i) it is a party to the Strasbourg Convention, or (ii) it is not a signatory of the Strasbourg Convention but its legislation is sufficiently developed to ensure the relevant protection of personal data and the state is included on a list approved by the DPA. As of the date hereof, the list of states granting the 'adequate protection' of personal data is adopted by DPA and consists of 19 countries, such as Canada, New Zealand, Israel, Switzerland, etc.

Personal data can also be transferred to third countries, even if the 'adequacy' conditions are not met. However, in this case, it is necessary to obtain 'qualified consent' from the relevant person comprising the elements referenced in section 6 above.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?
A group company is regarded as a third party. As above, it would either need to independently satisfy the legal requirements for processing personal data, or the data privacy consent provided to the 'original' data controller should contain consent to the processing / transfer between the group companies, and the relevant companies should enter into a written data transfer agreement.

10. When collecting personal data, what information needs to be given, and how?
Before the commencement of data processing the data controller, upon the request of the relevant person, should provide the relevant person with clear and detailed information regarding all the circumstances in relation to data processing, including:

(a) confirmation that his/her personal data is processed by the data controller
(b) the legal grounds and purposes for processing the personal data
(c) the purposes and methods of processing personal data used by the data controller
(d) the name and the address of the data controller, information on persons (except for the data controller's employees) who may access the personal data or persons to whom personal data can be disclosed under the agreement with the data controller or in accordance to the law
(e) a list of personal data processed referring to the corresponding subject of personal data, the sources from which the personal data were obtained, unless another way of obtaining the data is not allowed by the law
(f) the duration of processing and storing the personal data
(g) the procedure for enforcement by the relevant person of his/her rights, provided by the law
(h) information on performed or intended cross-border transfers of personal data
(i) the name and address of the technical processor of personal data, if the personal data processing is assigned or will be assigned to such person
(j) other information required under the law.

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?
The Data Protection Act does not specify the language of the consents which should be obtained in connection with data processing. However, according to the Data Protection Act the given consent should be concrete, informed and conscious, so that the relevant person fully understands the essence of giving consent. For this reason, in practice, it may be necessary to have a Russian translation of the consent. This will also help avoid the risk that the consent could be considered void. Thus bilingual consent is recommended.

12. What are the specific rules where the data controller has appointed a third party to process personal data?
The data controller may entrust the processing of personal data to a third party. The processing of personal data on the demand of a data controller should be performed on the basis of the relevant agreement, which should contain the elements required by the Data Protection Act. A company that processes personal data (the 'technical processor') should perform its activity in accordance with the requirements of the law, which includes ensuring the confidentiality and protection of the personal data.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?
Personal data may be processed to the extent and the duration necessary to achieve the purpose of the processing. Any document containing personal data must be destroyed when no further legitimate grounds to retain the data can be proved; unless the person whose personal data is stored/recorded has authorised the further storage/recording of the data or such authorisation is provided by law.

In accordance with the recent amendments introduced to the Data Protection Act, the duration of processing personal data may be provided not only in the law, but also agreed in an agreement. The Data Protection Act does not provide any time limitations for processing personal data. For example, it may be agreed with an employee that his/her personal data may be stored by an employer for a certain period of time after he/she leaves the company.

14. Specify below the mandatory technical, organisational or security measures.

As regards security measures, the Data Protection Act has implemented the provisions of Article 7 of the Strasbourg Convention (*Data Security*). Personal data must be protected against unauthorised access, alteration, transfer, disclosure by transfer or deletion as well as damage and accidental destruction. In order to ensure the security of personal data, the data controller should use technical devices certified by the Russian authorities. Certification procedures for technical devices are established by specialised state services (Federal Service for Defence or Federal Service for Technical and Export Control) and vary depending on the type of device and the level of protection ensured by the respective device. The data controllers are also obliged to keep a record of devices on which personal data are stored (the form of such record is not specified by the Data Protection Act). The data controller should also determine the level of damage which may be caused in the case of unauthorised processing of personal data. It is also necessary for the personal data controller to establish the rules of access to personal data etc.

The Data Protection Act does not provide further details on the technical and organisational measures mentioned above. Information on some of the requirements is provided in the relevant by-laws. However, many gaps in the regulations remain. Currently the relevant by-laws are being completed and amended.

15. Does a data controller have any other specific obligations?

A personal data controller must perform an internal audit and assessment of the effectiveness of measures which are taken to protect personal data. The personal data controller must also retain control over such measures and the level of protection of personal data. The Data Protection Act does not specify the contents and procedure for the audit. A Government Decree, adopted on 1 November 2012, provides that the audit may be performed by the data controller on its own or entrusted to an external company that specialises in the technical protection of confidential information. The Government Decree requires that an audit is performed at least once every three years.

16. What are the registration obligations at the DPA?

Data controllers must submit a notification to the DPA on their intent to process personal data. The notification procedure requires the completion of standard online and/or paper forms which is currently free of charge, and does not require the submission of additional documents (e.g. the data transfer agreements). In principle, data processing can commence only if a data controller has been registered. The DPA makes the registration within 30 days. After that the information on the personal data controller appears in the relevant register, which is accessible online. The information submitted by the data controller for notification must include information on the registration details of the controller, the purposes of the personal data processing, the list of personal data, description of measures taken by the controller to ensure the security of personal data, cross-border transfers of personal data etc. If any changes are made to the registration data, an application for the registration of changes must be submitted to the DPA. The registry of personal data controllers is available for inspection at the following address: www.pd.rsoc.ru/controllers-registry/

17. Are there any exemptions from the registration obligation?

No notification to the DPA is required in the case of processing the following personal data:

(a) personal data of employees processed by an employer for employment purposes
(b) personal data received by a data controller in connection to entering into an agreement with the respective person, under the condition that personal data is not disclosed to third parties and is used only for the purposes of executing the respective agreement

(c) personal data of members of a public union or religious organisation, processed by these unions and organisations for the purposes of their activity, under the condition that the personal data is not disclosed to third parties
(d) personal data made public by the relevant person
(e) personal data which includes only names, surnames and patronymic names of the relevant persons
(f) personal data which is necessary for the organisation of a one-time entry of the relevant person to the territory of the controller (or for the similar purposes)
(g) personal data which is included in information systems for personal data and that have the status of state automatic information systems and in state information systems for personal data, created for the purposes of the protection of state security and public order
(h) personal data processed without the use of automatic methods, in compliance with the law or
(i) personal data processed in accordance with regulations on transport security.

18. Are there any specific notification obligations?
The notification obligations provided by the Data Protection Act are the same for all types of personal data controllers. The Data Protection Act does not provide for any particular notification obligations for particular categories of controllers.

19. Does the relevant person have the right to access, rectify, remove or block their personal data?
In line with Article 8 (*Additional safeguards for the data subject*) of the Strasbourg Convention, the relevant person has the following rights:

Information
The relevant person may request information about processing his/her personal data, including confirmation that his/her personal data is processed, the legal basis, purpose and methods of processing, the name and address of the data controller, information on third parties with access to the personal data, a list of the personal data being processed and the source of their collection, the duration of processing (including duration of storage), information on cross-border transfers of personal data, information on the technical processor of personal data, on the procedure for the relevant person to realise of his/her rights provided under the Data Protection Act. The data controller must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days.

Rectification
Data controllers must rectify all personal data if it is false.

Deletion
Personal data must be deleted (with the exception of data processed on the basis of law) in the following cases:
(a) upon the request of the relevant person
(b) if the personal data is deficient, outdated, inaccurate, or illegally obtained and is not necessary for the declared purpose of processing
(c) if the purpose of processing is achieved, or the purpose is no longer relevant.

Blocking
If processing of personal data is found to be illegal, if the processed data is deficient or inaccurate, or upon the request of the relevant person, the personal data controller must block the relevant personal data or make sure that they are blocked.

The controller should also block the relevant personal data if it becomes impossible to delete it within the relevant period. Such data, however, should be deleted within a period of six months, unless another period is provided for by the law.

Appealing to the DPA or to court

The relevant person may also appeal to the DPA or a court in case of the unlawful processing of his/her personal data.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?

(A) Administrative remedies and other sanctions

In the case of a violation of the provisions of the Data Protection Act, the DPA and/or the relevant court are entitled to the following:

(a) to request the personal data controller to rectify the violation of personal data processing or
(b) to issue a warning to the personal data controller
(c) to impose the following fines for violations of personal data processing:
   - RUB 300 – 500 (€7.5 – 12.5) on individuals
   - RUB 500 – 1000 (€12.5 – 25) on officials of legal entities
   - RUB 1000 – 5000 (€25 – 125) on legal entities

Draft amendments to the laws which aim at substantially increasing the fines are currently under discussion.

(B) Judicial remedies

In accordance with Article 10 of the Strasbourg Convention (*Sanctions and Remedies*), the Data Protection Act enables a relevant person to file for a court action against a controller, and in particular, to seek compensation for damage caused as a result of the illegal treatment of personal data.

(C) Criminal law issues

In serious cases, unlawful data processing may also be deemed as illegal collection and distribution of information on the private life of a person, which constitutes a private or family secret. Under Article 137 of the Russian Criminal Code, such violations may be punished with a fine, compulsory work or imprisonment.

Slovakia

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?
Act No. 122/2013 Coll. On the Protection of Personal Data ("Data Protection Act") is based on Directive 95/46/EC and sets the general framework for data protection. Regulation No. 164/2013 on the scope and documentation of the security measures and regulation No. 165/2013 on the examination of the data protection official are also applicable.

To be more precise, the Data Protection Act defines the protection of personal data of natural persons in the course of their processing, principles of personal data processing, security of personal data, protection of the rights of individuals, trans-border data flows, registration and keeping of records of filing systems databases. The Data Protection Act can be found at the following link: http://www.dataprotection.gov.sk/buxus/docs/122_2013.pdf (only in Slovak at this stage).

The Data Protection Act applies to anyone that processes personal data, determines the purpose and means of processing or provides personal data for their processing.

The Data Protection Act also applies to controllers, who do not have their registered office or permanent residence in:

a) the Slovak Republic but are located abroad where the laws of the Slovak Republic take precedence based on international public law,
b) a Member State of the European Union, provided that for the purposes of personal data processing they use fully or partially automated means or other than automated means of processing located in the Slovak Republic, while such means of processing are not used solely for the transfer of personal data through Member States of the European Union.

2. What is the data privacy authority ("DPA") in your country?
The supervisory authority established in accordance with Article 28 of Directive 95/46/EC is The Office for personal data protection of the Slovak republic (further as "DPA"). Its website can be found at http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=92

3. Does an internal data privacy officer or similar need to be appointed?
Data controllers are responsible for the internal supervision and protection of processed personal data. Only a natural person enjoying full legal capacity, who meets the precondition of integrity and passes the relevant exams, may perform the function of a personal data protection officer. A natural person, who is a statutory authority of the controller and a natural person entitled to act on behalf of the statutory authority of the controller, cannot perform the function of the personal data protection officer.

If more than 20 entitled persons are processing data at the controller, he shall authorize a personal data protection officer in writing for the internal supervision of compliance with the Data Protection Act. In case a controller is processing personal data by less than 20 entitled persons, he must register the filing system in which personal data are processed. (If the data protection officer is appointed, the registration is not required.) If the controller is processing the personal data by more than 20 entitled persons, the controller has to authorise a personal data protection officer within 60 days from the day he starts with processing of personal data in the filing system. The data protection official must pass the exams at the DPA.

The voluntary appointment of a data protection officer is no longer possible.

An entitled person is any natural person comes into contact with personal data within the framework of his employment relationship, civil service employment relationship, civil service relationship, membership, based on an authorisation, election or appointment or in relation to holding public office, who may process personal data at the controller or processor.

The basic duties of the personal data protection officer are to assess whether there is any risk that the rights and freedoms of data subjects may be violated, and to notify the controller of any violation of the rights and freedoms of individuals, to implement the technical, organisational and personal measures, to carry out internal supervision to monitor the fulfilment of the controller's basic obligations and to internally supervise trans-border personal data flow, to register/change/deregister relevant databases etc.

A controller who authorized a personal data protection officer has to register such person with the DPA within 30 days from the day of the authorization.

4. Do most companies have internal privacy policies and external privacy notices?
It is common for companies, especially multinational companies who process cross-border data flows both within and outside their company group, to introduce internal privacy policies and publish privacy notices.

5. What shall be deemed as "personal data"?
Similarly to Directive 95/46/EC, the Data Protection Act does not provide for an exhaustive list of data which shall be deemed as "personal data", therefore this shall be assessed on a case-by-case basis. The Data Protection Act only provides a general definition of personal data. Personal data shall mean any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier of general identifier or by reference to one or more factors specific to his physical, physiological, psychic, mental, economic, cultural or social identity.

In line with Article 8 of Directive 95/46/EC, the Data Protection Act sets forth a special category of data ("sensitive personal data"), i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or movements, trade-union membership, and data concerning health or sex life. Further when processing personal data, a birth number may be used only for the purposes of identification of a natural person provided that its use is necessary for achieving the given purpose of the processing.

Personal data relating to a breach of provisions of the criminal law, misdemeanours act or civil law, or relating to execution of final judgements or decisions, may only be processed by a person entitled to do so by a special act, e.g. data processing by the police. Biometric data may be processed only if the processing of such data is carried out for an appropriate purpose and it is necessary to achieve such purpose, and such processing expressly results for the controller from the special act, or consent has been granted by the data subject for such processing, or if it is necessary for the performance of a contract to which the data subject is a party, or if the processing is necessary to protect the statutory rights and legitimate interests of the controller or the third party.

Personal data relating to the mental identity of a natural person or his mental capacity to work may only be processed by a psychologist.

6. Is it necessary to obtain consent from the relevant person in order to be able to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?
The definition of personal data processing is very broad. The processing of personal data means any operation or set of operations which is performed upon personal data such as obtaining, collection, recording, organization, adaptation or alteration, retrieval, consultation, alignment, combination, transfer, use, storage, destruction, transmission, provision, making available or making public.

Personal data may be processed with the prior consent of the data subject, or if the processing of personal data is permitted by law. The data subject's consent means only a freely given specific and informed indication of his wishes by which the data subject knowingly signifies his agreement to personal data related to him being processed. In practice, the consent can be given verbally, in writing, or electronically. Electronic acceptance may be in the form of the relevant person clicking an "acceptance button" or ticking a "consent box". Prior to expressing acceptance by electronic means, the relevant person should also be given an opportunity to read the relevant privacy policy.

Even though written consent is not a must, the data controller should always be in a position to prove (in case of

any ambiguity) that consent was provided properly and lawfully so proper archiving is advisable. It is also worth noting that in line with Article 5(3) of Directive 2002/58/EC, data processors or controllers may only place cookies (or similar technologies) on computers of users with their prior consent. The consent also means that the user will accept the cookies by a respective setting of the web browser

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?

On the basis of Article 7 (b) to (f) of Directive 95/46/EC, personal data can be processed without consent, if:

a) the data are processed pursuant to a special act (e.g. the act on health insurance, the act on banks, etc.), international treaty binding for the Slovak Republic or directly enforceable legally binding act of the European Union stipulating a list of personal data, the purpose of their processing and the group of data subjects;
b) the processing of personal data is necessary for the purpose of artistic or literary expression, for the purpose of informing the public by means of mass media and if the personal data are processed by a controller for whom it is necessary under the scope of his activities;
c) the processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to establish relations of the data subject prior to entering into a contract, or in case of negotiation of the contract at the request of the data subject;
d) the processing of personal data is necessary for the protection of life, health or property of the data subject;
e) the subject of the processing is constituted solely by the title, name, surname and address of the data subject without a possibility of adding his other personal data and they are to be used solely for the controller's needs concerning mail correspondence with the data subject and the keeping of records of such data; if the scope of the controller's activities is direct marketing, he may provide the above personal data, without a possibility of making them available and public only if they are to be provided to another controller whose scope of activities is also solely for the purposes of direct marketing and the data subject did not file an objection;
f) the processed personal data have already been made public legally;
g) the processing of personal data is necessary for the fulfilment of an important task carried out in the public interest; or
h) the processing of personal data is 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 and by their conduct they do not violate his right to the protection of his personal rights and privacy.

In the above cases, personal data may also be processed if the relevant person withdraws the consent to data processing (which can be done at any time under the law). The above exception may apply for example in cases where personal data is necessary to perform an employment contract from the data controller's side, e.g: when data is provided to the company calculating wages, which is considered a processor. In such a case, if the controller engages the processor with the processing of personal data, the processor must inform the data subject about the fact that he is processing his/her personal data. Also the controller should inform the data subjects of this fact during the next contact, however, not later than within three months from the day of the engagement of the processor, if the data subject is not informed by the processor within this time period.

8. Can the personal data be transferred to another country? On what conditions? Are there any restrictions to the exporting of any personal data (e.g. nature, purpose, country, specific measures)?

The transfer of data to a member state of the EU has the same regime as if data was transferred within the Slovak Republic.

Personal data may be transferred to a third country, which, based on a decision of the European Commission, ensures an adequate level of protection.

Where the country of final destination does not ensure an adequate level of protection, the transfer may be executed only on the condition that:

a) the controller has adopted the EC Model Clauses, or the Binding Corporate Rules
b) the data subject consented to it, while knowing that the country of final destination does not ensure an adequate level of protection,
c) it is necessary for the performance of a contract between the data subject and the controller or for the negotiation of changes to the contract with the data subject, or for the establishment of pre-contractual measures upon the data subject's request,
d) it is necessary to enter into, or for the performance of, a contract concluded by the controller in the interest of the data subject with another entity,
e) it is necessary for the protection of the data subject's vital interests,
f) the transfer is necessary or required by law to safeguard an important public interest or for the establishment, implementation, or defense of legal claims arising by the operation of law or international treaty by which the Slovak Republic is bound,
g) the transfer relates to personal data, which are part of lists, or registers according to a special laws and are publicly available or made available to those who demonstrate a legal basis for the disclosure, subject to the conditions stipulated by law.

Based on the Data Protection Act, the processor shall be entitled to process personal data only to the extent and under conditions agreed upon with the controller, or with another processor, provided that the controller expresses its consent in a written transfer agreement.

If the personal data are to be transferred to a country outside the EU and EC Model Clauses are incorporated in the transfer agreements with the processor or controller seated in the third country, or if the transfer will be executed based on the Binding Corporate Rules, the transfer does not need to be approved by the DPA. This also applies in case the country of final destination is the US and the importer has joined the Safe Harbour programme and in the transfer agreement the required elements under the Data Protection Act are included, which are: i) identification data of the contractual parties, ii) the purpose of transfer of personal data, iii) the processing operations in the third country, iv) a list of personal data, v) a list of data subjects, vi) the time of processing of personal data.

In all other cases, the DPA's prior approval of such transfer is needed. The application for such consent has to contain the identification data of the exporter and importer, the purpose of transferring data, the identification of data subjects, categories of transferred data, and the time for which the data will be stored by the importer. The transfer agreement must be attached to the notification. The DPA has 30 days to decide.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?

A group company is regarded as a third party, and, as above, would either need to independently satisfy the legal requirements for processing personal data, or (the data privacy consent provided to the "original" data controller would have to contain consent to the processing / transfer among the group companies and the relevant companies should enter into a written data transfer agreement as well. If the transfer agreement contains the EC Model Clauses, or the Binding Corporate Rules were adopted, or the importer joined Safe Harbour and the transfer agreement meets the requirements under the Data Protection Act, the consent of the DPA for the transfer is not required.

10. When collecting personal data, what information needs to be given, and how?

A controller who intends to obtain personal data from a data subject must inform the data subject, at the latest while obtaining the data, and notify him in advance of the following without being requested:

a) identification data of the controller;
b) identification data of the processor;
c) the purpose of the personal data processing;
d) the list of processed personal data;
e) identification of the person entitled to obtain the personal data;
f) advice on voluntariness or obligation to provide the requested personal data;
g) third parties, provided that it is expected or clear that personal data will be provided to (and further processed by) them;
h) group of recipients, provided that it is expected or clear that personal data will be made available to (but not processed by) them;
i) form of making the data public, provided that personal data are to be made public;
j) third countries, provided that it is expected or clear that personal data will be transmitted to these countries;
k) advice on the existence of the data subject's rights.

Usually this information is provided to the data subject while obtaining the consent for the processing of personal data directly in the text of the consent. This information

may be provided to data subjects also through the web page of the data controller.

11. What are the notice & consent language requirements (particularly, whether English language would be deemed sufficient or if translation into the local language would be required)?

The Data Protection Act does not specify the language of the notices and consents in connection with data processing so the English language would be deemed sufficient; it is not mandatory to translate such documents to the local language. However, in case of any ambiguity, the data controller must prove that the relevant person understood the language of the notice & consent, so bilingual documents are recommended.

12. What are the specific rules where the data controller has appointed a third party to process personal data?
Each controller may authorise a processor in a written contract to process personal data. Such processor may process personal data only to the extent and under the conditions agreed upon with the controller in a written contract. The requirements of such contract are specified in the Data Protection Act. If the controller engaged the processor with the processing after acquiring personal data he should inform the data subjects of this fact during the next contact, however, not later than three months from the day of tasking the processor, if the processor does not inform the data subject itself. This shall also apply if data processing is taken over by another controller, e.g. in case of a merger of two controllers.

The processor shall inform data subjects that he was authorised by the controller to process the personal data of data subjects during the next contact with them.
In case personal data is to be provided to another controller, and the previous controller will not cease to exist, personal data may be provided to such controller only if the data subjects gave consent for such provision.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?
In line with Article 6 of Directive 95/46/EC, personal data may be processed to the extent and the duration necessary to achieve the purpose of the processing. Any documents containing personal data must be destroyed when no further legitimate grounds for such data can be proved, unless the person whose personal data is stored/recorded has authorized the further storage/recording of such data or such authorization is provided by law.

As regards the specific archiving rules, it is advisable to retain data until the relevant period of limitation has expired. A number of circumstances can make it difficult to establish the date on which this period expires and there are also a couple of rules arising under the laws which regulate various specific retention obligations in connection with specific documents (e.g. general period of limitation for civil law claims, employment related documents, safe-keeping of accounting documents and tax returns, employer's certificate concerning social security and workplace accident allowance, declaration on social security entitlement etc.) Any concerns regarding the retention obligation pertaining to a particular document shall be assessed on a case-by-case basis.

14. Specify below the mandatory technical, organizational or security measures.
As regards the security measures, the Data Protection Act has implemented the provisions of Section VIII of Directive 95/46/EC (Confidentiality and Security of Processing). Personal data must be protected against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and publication, as well as against any

other unauthorized forms of processing. Both the controller and the processor shall be responsible for the security of personal data and both have to apply due technical, organisational and personal measures adequate to the manner of processing.
Regulation No. 164/2013 on the scope and documentation of the security measures lists the relevant technical, organisational and personal measures (please find some examples below).

In order to protect data processed in various databases it must be ensured with adequate technical devices that the data stored in databases cannot, unless permitted by law, be directly linked to each other and traced back to the relevant persons.

Under the regulation, the following measures are considered as adequate: storage of documentation in locked cases, using passwords to PCs, proper configuration of PCs, using a firewall, advising the employees who are responsible for the processing of personal data at the employer about the rights and obligations stipulated in the Data Protection Act and of the liability for their breach, conclusion of confidentiality agreements, etc. In some cases, e.g. if special categories of personal data are processed and the computer on which such data are stored is connected to the internet, the controller and processor have to develop a Security Project. The Security Project is a higher standard of documentation of the adopted measures. It has mandatory contents and consists of i) the name of the filing system(database), ii) security policy, iii) analysis of the filing system's security, iv) and security directives.

15. Are there any other specific obligations of the data controller?
The controller is obliged to:
a) determine the purpose of the processing of personal data before starting the processing of personal data;
b) determine the means and manner of the processing of personal data;
c) obtain personal data solely for a defined or determined purpose;
d) ensure that only such personal data are processed, the extent and contents of which correspond with the purpose of their processing and are necessary for its achieving;
e) obtain personal data separately for various purposes and ensure that personal data are processed and used solely in the manner adequate to the purpose for which they were collected;
f) process only accurate, complete and up-to-date personal data; the controller shall be obliged to block inaccurate and incomplete personal data and rectify or complete them without undue delay; inaccurate or incomplete data that cannot be rectified or completed in order to make them accurate and complete shall be clearly marked by the controller and destroyed as soon as possible;
g) ensure that the collected personal data are processed in a manner enabling the identification of data subjects only during a time period necessary for achieving the purpose of processing;
h) destroy the personal data whose purpose of processing has expired;
i) keep a record of the filing systems on his own, in case if filing system does not need to be registered.

16. What are the registration obligations at the DPA?
The controller shall submit the filing system for registration, if applicable before commencement of the processing of personal data in the filing system. The registration procedure requires the completion of the standard form of DPA. The fee for the registration of the filing system is EUR 20.

Assignment of a registration number to the filing system and issuance of a confirmation of its registration shall constitute a part of the registration. The controller may start to process the personal data in such filing system upon the delivery of the registration form to DPA.

In case of special registration, e.g. in case of transferring of sensitive data to third country not ensuring adequate level of protection, the filing system in which such data are stored must be firstly registered. The data transfer can be commenced only if the registration is made.

17. Are there any exemptions from the registration obligation?
Yes, the Data Protection Act specifies what kind of filing systems have to be registered.

The obligation to register shall apply to all filing systems, in which personal data are processed by fully or partially automated means of processing, except for filing systems:
a) which are subject to special registration (see below);
b) which are subject to internal supervision of a personal data protection officer, which was authorized by the controller in writing;
c) containing personal data concerning membership of persons in trade-union organisations, religious associations or political parties and if these personal data are processed by these organisations and used solely for their internal needs;
d) containing personal data that are processed pursuant to a special act, international treaty binding for the Slovak Republic or directly enforceable legally binding act of the European Union.

Special registration shall apply to filing systems in which the controller processes:
a) at least one of the sensitive personal data, and at the same time their transfer to a third country not ensuring an adequate level of protection is expected or executed;
b) personal data, whose processing is necessary for the protection of statutory rights and legitimate interest of the controller;
c) biometric personal data.

The controller must submit a filing system for special registration at the DPA before commencing the processing of personal data. The assignment of a registration number to the filing system and the issuance of a confirmation of its registration constitutes a part of the special registration; the controller may commence the processing of personal data in the filing system submitted for special registration the day after receiving confirmation of its registration. The fee for special registration of a filing system is 50 EUR.

18. Are there any specific notification obligations?
N/A

19. Does relevant person have rights to access, rectify, remove or block their personal data?
In line with Article 12 (Right of access) of Directive 95/46/EC, the relevant data subject has the right to request from the controller:

Information and Rectification

a) information about the state of the processing of his personal data in the filing system, and if personal data about the data subject are processed or not;
b) exact information, in a generally intelligible form, about the source from which the controller obtained his personal data for their processing;
c) a copy of his personal data, in a generally intelligible form, which constitute the subject of the processing;
d) rectification of inaccurate, incomplete or not updated information, which constitute the subject of the processing;
e) destruction of his personal data and returning of the documentation containing the personal data, provided that the purpose of their processing was fulfilled;
f) destruction of his personal data, which constitute the subject of the processing, provided that the law was breached.

The controller shall satisfy the requests of the data subject under letters a), b), d) to f) free of charge. The information under letter c) is provided free of charge to the data subject, except for a fee in the amount not exceeding the amount of material costs accrued in connection with the making of copies, providing technical carriers and sending the information to the data subject.

The controller shall satisfy the requests of the data subject and notify him in writing at the latest within 30 days from the day of their receipt.

Objection

The data subject shall be entitled to object to the controller's, upon a free-of-charge written application:

a) processing and using his personal data for the purposes of direct marketing;
b) processing of personal data if the personal data are processed without the consent of the data subject if it is permitted because of the exceptions as stated above. The data subject should state the the legitimate reasons of an infringement of his rights and legitimate interests or shall submit the evidence of an infringement of his rights and legitimate interests that are or can 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 the controller shall be obliged to block the personal data, the processing of which was objected by the data subject without undue delay and the controller has to destroy them as soon as possible
c) to object and refuse the decision of the controller which may have for the data subject the significant implication, if such decision was made only based on the automatic processing.

Deletion

After the purpose of processing is fulfilled, the controller shall destroy the personal data without undue delay.

The controller shall destroy personal data, without undue delay also if:

a) the reasons which prevented the obtaining of a consent of the data subject ceased to exist and the consent was not given (is permitted in case the processing of personal data is necessary to protect the life, health or property of data subject) ;
b) the controller is processing incorrect or inaccurate personal data;
c) the data subject filed an objection to the personal data being processed for the purposes of direct marketing.

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.

Blocking

The basic duty of the controller is to process only accurate, complete and, where necessary, updated personal data in respect of the purpose of their processing; the controller shall be obliged to block inaccurate and incomplete personal data and rectify or complete them without undue delay. If personal data of a data subject are processed without the data subject's consent, the data subject may object to such processing in case the processing infringes his rights and legitimate interests. If it is proved that the objection of the data subject is valid and legitimate reasons do not prevent it, the controller shall be obliged to 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.

If the consent of the data subject for the processing of his/her personal data was withdrawn before the lapse of its validity, the controller has to block his/her personal data.

Turning to the DPA or to a court

The relevant person may also turn to the DPA or a court in case of the unlawful processing of his/her personal data.

20. What are the sanctions for infringement of the obligations by data controller (i.e. fines, criminal liability, civil liability, or any other)?

(A) Administrative remedies and other sanctions
In case of a violation of the Data Protection Act by the controller or processor, the DPO may:

a) impose an obligation to take, in a determined time limit, the technical, organisational and personal measures adequate to the manner of the processing;
b) prohibit the processing of the personal data, the processing of which is contrary to the provisions of the Data Protection Act;
c) order the removal or destruction of the personal data in a determined time limit, provided that they are or were processed illegitimately;
d) impose on the controller an obligation to change the processor;
e) impose an obligation to develop or to update the security project or documentation;
f) make public the business name or name, registered office or permanent residence, identification number, the corporate form of the person, who committed the illegal action and the verdict of an enforceable order, the grounds of the order and characteristics of the facts of the case concerning the breach of protection of personal data;
g) impose a fine of EUR 300 up to EUR 300,000 (as the case may be).

The DPA may impose a fine repeatedly, provided that the obligation was not fulfilled in a determined time limit.
A fine may be imposed within two years from the day the DPA determined the breach of the obligation, but at the latest within three years from the day the obligation was breached.

(B) Judicial remedies
In accordance with Article 22 of Directive 95/46/EC (Remedies), the Data Protection Act enables the relevant person to file for court action against the controller.

(C) Criminal law issues
In serious cases, unlawful data processing may also be deemed as, "Unauthorised Use of Personal Data", "Violation of the Privacy of Correspondence" or "Abuse of foreign rights" under Act No. 300/2005 Coll. Criminal Code which may also be punished by imprisonment.

Ukraine

1. What is the general data privacy law that applies to the collection, processing, disclosure or exporting of personal data in your country? What is the scope of application of the Data Protection Act? What specific obligations in the law, if any, apply outside of its jurisdiction?

The Ukrainian Law on Personal Data Protection N 2297-VI of 1 June 2010 (further – the 'Data Protection Act') is the principal legal act that regulates personal data processing in Ukraine. The Data Protection Act can be found *in Ukrainian* at the following link: zakon2.rada.gov.ua/laws/show/2297-17. There are also several regulations which contain sector-specific privacy and security requirements (e.g. those that apply to the banking sector).

In addition to the Data Protection Act, the Ukrainian Parliament ratified the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data that forms an integral part of national legislation starting from 6 July 2010.

The Data Protection Act aims to protect personal data during the process of collection, accumulation, processing and use for purposes other than private and/or certain professional circumstances. Therefore, any aspects of personal data processing that take place in Ukraine, including cross-border transfer of personal data, is within the ambit of the Data Protection Act.

2. What is the data privacy authority (DPA) in your country?

The Data Protection Act sets out a requirement for a special authority to supervise compliance with its provisions. Such an authority was established by the President's Order (1085/2010) on 9 December 2010. Under the Order, the State Service of Ukraine for Personal Data Protection (in Ukrainian – *Державна служба України з питань захисту персональних даних,* further – the 'Agency') is a central governmental body in the domain of personal data protection in Ukraine. Its website can be found at zpd.gov.ua/.

Starting 01 January 2014, the state agency in charge of personal data protection matters in Ukraine will change. The Agency is to be abolished and its functions will be transferred to the Ombudsmen (in Ukrainian – *Уповноважений Верховної Ради України з прав людини).*

3. Does an internal data privacy officer or similar need to be appointed?

By law, all data controllers and processors must appoint an officer or establish a structural subdivision that will be responsible for processing personal data within an organisation.

No specific requirements are set by law as regards the qualifications or professional experience of individuals who can be appointed as responsible officers. Only a general requirement applies according to which a responsible officer must be a person appointed in accordance with his/her service, labour or professional duties.

Alternatively, instead of appointing a responsible officer, a data processor or controller may establish a separate structural subdivision to take care of data protection matters. This separate subdivision would be a separate structural unit of the data controller or processor (e.g. affiliate) and would perform its function on the basis of the relevant internal policy/regulation.

An officer or structural subdivision responsible for data protection performs the following functions:

(i) ensuring that all employees of the database controller and processor familiarise themselves with the statutory requirements as regards personal data protection, in particular, their duty to prevent the disclosure in any way whatsoever of the personal data that they were entrusted with or that they became aware of in connection with performing their professional, official and employment duties
(ii) managing personal data processing by employees of the database controller and processor in line with their professional, official and employment duties to the extent necessary to perform such duties
(iii) managing the processing of requests to access personal data from subjects involved in personal data processing
(iv) providing relevant persons with access to their own personal data
(v) informing the managers of the database controller and processor of measures to be taken to bring the content of the personal data and personal data processing procedures into compliance with the law
(vi) informing the managers of the database controller and processor of violations of personal data processing procedures.

4. Do most companies have internal privacy policies and external privacy notices?

Although internal privacy policy or external privacy notices are not required by law, many companies, especially multinational ones, develop such documents.

5. What is deemed as 'personal data'?

The Data Protection Act defines personal data as data, or a combination of data, relating to an identified or specifically identifiable natural person.

The Data Protection Act explicitly prohibits processing certain sensitive personal data, i.e. data which relates to racial or ethnic origin, political, religious or philosophical beliefs, political-party or trade-union membership, as well as data concerning the health or sex life of the relevant persons.

However, the Data Protection Act also provides for exemptions from this rule. Some exemptions mirror those set out in the EU Data Protection Directive (95/46/EC) (e.g. explicit consent of the relevant person to processing his/her sensitive personal data), although the Data Protection Act offers some additional grounds for exemption from restrictions on processing sensitive data. In particular, restrictions do not apply to cases where the processing of personal data concerns:

(i) accusations of committing crimes
(ii) rulings of the courts
(iii) state authorities' fulfilment of their duties related to anti-terrorism, counter-intelligence or police investigative activity, or when the personal data was made publicly available by the relevant person.

6. Is it necessary to obtain consent from the relevant person in order to process personal data, or to transfer such personal data to third parties? Are there special requirements for processing certain categories of data (e.g. contracting parties, employees, patients etc.)?

Generally, a data controller must always obtain explicit informed consent from the relevant person in order to process his/her personal data.

The Data Protection Act provides that consent may be granted in writing or in any other identifiable form. If the consent is obtained through electronic communication, the data controller or processor should use web resources that can confirm that consent was obtained in order to comply with the 'identifiable form' requirement.

Although starting 01 January 2014 the 'identifiable form' requirement will be removed from the Data Protection Act, we recommend following it in practise to minimise a risk of the consent being questioner.

The Data Protection Act also sets out mandatory requirements regarding the content of the consent. Specifically, it must contain: (i) the name of the data controller to whom the consent for data processing is given; (ii) the exact amount of the personal data to be processed; (iii) the precise purpose of processing the personal data (if the purpose of processing changes, it is necessary for the relevant persons to grant their consent to processing for the changed purpose); (iv) the term for which the data will be processed and (v) any requirements for the transfer of the relevant person's personal data to third parties.

The requirement to provide consent for personal data processing is common for all types of data.

7. Are there any exceptions under which personal data can be processed or transferred to third parties without the relevant person's consent?

Processing personal data without the relevant person's consent is permitted only in exceptional cases specifically provided for by law and only (if necessary) in the interests of national security, economic wellbeing and protection of human rights. Further, the law permits personal data processing without the relevant person's consent if processing is necessary to protect his/her vital interests (in any case such processing is possible only until the relevant person's consent can be obtained).

Third party access to personal data should be regulated by the terms and conditions of the relevant persons' consent. If the consent covers the possibility of the data controller providing access to third parties, then provision of such access will be in line with the Data Protection Act, and vice versa.

8. Can personal data be transferred to another country? On what conditions? Are there any restrictions on exporting any personal data (e.g. nature, purpose, country, specific measures)?

The Data Protection Act sets out a general rule that personal data may be transferred only to states that ensure adequate data protection. Such states include EEA countries and countries that ratified the Convention of the Council of Europe on Protection of Persons in Connection with Automated Personal Data Processing. A complete (expanded) list of the countries that provide adequate protection of personal data is being produced by the Ukrainian government.

In addition to the adequate protection requirement, cross-border transfers of personal data are possible only if one of the following conditions is met:

(i) the relevant person has granted his/her express consent to such transfer
(ii) the data controller and a relevant person need to enter into or perform an agreement for the benefit of the relevant person
(iii) the data transfer is necessary to protect the vital interests of the relevant person
(iv) the data transfer is necessary to protect the public interest or pursue legal remedies
(v) the data controller has provided relevant guarantees to protect the relevant person's privacy.

The Data Protection Act additionally prohibits the transfer of personal data (including cross-border transfers) for any purpose other than the purpose for which the data was originally collected.

9. Are there different requirements or treatment if the third party processing the personal data belongs to the same company group, or if it is an external company?

Ukrainian law provides the same requirements with respect to processing personal data by third parties that belong to the same group (intra-group processing) and those that are external companies. Thus, a group company is regarded as a third party by the Data Protection Act and needs to either (i) obtain the relevant person's consent independently or (ii) be covered by the third party consent issued to another company of that group (which consent explicitly allows the intra-group transfer of the data) and enter into the relevant agreement with the company to whom the consent has been granted (the data controller).

10. When collecting personal data, what information needs to be given, and how?

Before obtaining a person's consent to process his/her personal data, a data controller or data processor must inform that person of the purpose of the data processing.

Furthermore, in accordance with the Data Protection Act, when collecting personal data upon the relevant person's consent, this person must be informed of the following:

(i) the identity of the personal data controller
(ii) the contents of the personal data being collected
(iii) his/her rights granted by the Data Protection Act
(iv) the purpose of the data collection
(v) the parties to whom his/her personal data is being transferred.

If personal data is being collected on grounds other than the relevant person's consent, the same information is provided the relevant person by the data controller or processor within ten business days of collecting the personal data (starting 01 January 2014 the term is extended to thirty business days).

11. What are the notice & consent language requirements (particularly, whether English would be deemed sufficient or if translation into the local language would be required)?

The Data Protection Act does not specify the language of notices and consents required in connection with data processing. Under general rules set out by Law of Ukraine 'On Basics of State Language Policy', in their economic and social activities, entities and organisations (other than those that belong to the public sector) are free to use Ukrainian or any other languages.

Therefore, consent may be provided in English, but it is highly recommended to have a parallel translation in Ukrainian in order to be able to prove to the Agency that the relevant person fully understood the conditions of consent and that the consent fully covers the scope and purpose of the data processing.

12. What are the specific rules where the data controller has appointed a third party to process personal data?

A data controller may appoint a third party to process personal data only if the relevant person has consented to it and only to the extent specifically provided by that consent or by law. The data processor may process personal data if it is expressly entitled to do so by law or by a relevant written agreement entered into with the data controller. Agreements between the data controller and data processor must clearly specify the scope and purpose of the data processing.

13. Are there any legal terms (maximum or minimum) for the retention or storing of personal data?

Under the Data Protection Act, personal data may be processed during the term specified by the relevant person's consent or by law, but for no longer than is required in order to achieve the legitimate purpose of the data processing.

Personal data must be destroyed in the following cases:

(i) expiry of the term for storing such data as provided for by the relevant person's consent or by law

(ii) termination of the legal relationship between the relevant person and the data controller/processor unless otherwise is provided by law
(iii) where there is a valid court judgement regarding withdrawal of the personal data from the database.

14. Specify below the mandatory technical, organisational or security measures.
Under the Data Protection Act, all parties to a data processing relationship (including data controllers and processors) must ensure the relevant data is protected from unauthorised processing and access.

The data controller is responsible for undertaking all necessary security measures to protect the data being processed in the database. For this purpose the data controller must determine/appoint:
(i) the location of the database
(ii) procedures for changing, supplementing, transferring, depersonalising and destroying the personal data being processed in the database
(iii) an officer or structural subdivision responsible for data processing
(iv) security measures to protect the data being processed.

A data controller may grant its employees different levels of access to the personal data being processed according to their professional, working or service duties.

Under Ukrainian law, data processing in computerised (automated) systems should include the following technical, organisational and security measures:
(i) use of network protection elements to prevent unauthorised access to the data
(ii) use of authorisation/identification procedures for employees of the data controller who may access the database
(iii) registration of the various processing procedures
(iv) installation of anti-virus software
(v) use of technical equipment to secure an uninterrupted energy supply to the computerised system in which the data is processed.

If personal data is processed in card files, the data controller must comply with the following requirements:
(i) documents containing personal data are to be formed into files depending on the purpose of the data processing
(ii) files with documents containing personal data must have internal descriptions of the documents indicating the purpose of processing and the category of personal data
(iii) card indices must be stored in rooms (cabinets, safes) protected against unauthorised access
(iv) doors to the rooms (cabinets, safes) must be equipped with a lock or access control.

Specific security requirements are set out by law with respect to data processing in certain sectors (e.g. banks).

15. Does a data controller have any other specific obligations?
A data controller must notify the relevant person of any transfers of his/her personal data to any third parties if such notification duty is required by the consent or by law. The notification must be made within ten business days of the relevant transfer.

Notification on the transfer of personal data is not required in the following cases:
(i) transfers of personal data upon requests arising from investigation and search operations or counter-intelligence tasks, counter-terrorism activities
(ii) performance by public authorities and local government bodies of their duties as provided by law

(iii) personal data processing for historical, statistical or scientific purposes
(iv) if the relevant person has already been provided with information on his/her personal data processing at the stage of data collection (see Section 10 above).

Further, a data controller must notify the relevant person if his/her personal data has been changed or deleted. The data controller must also notify the third parties to which the relevant personal data has been provided (including, as the case may be, a data processor, the Agency etc). The notification must be made within 10 (ten) business days of the change or deletion.

16. What are the registration obligations at the DPA?
The Data Protection Act, as in force at the date of this guide is published, provides for a mandatory requirement to register any database (with the exception of databases of employees, members of non-governmental and religious organisations, trade union memberships and political parties) with the State Register of Personal Data Databases (further – the 'Register').

The definition of database offered in the Data Protection Act is rather broad, and in practice, any combination of structured personal data – be it in electronic form or in an index – may be deemed to be a database.

The Data Protection Act requires every database to be registered in the Register by way of filing a relevant notice with the Agency.

The Data Protection Act further specifies certain information to be contained in the notice, including:
(i) a request to include the database in the Register
(ii) information regarding the personal data controller
(iii) information regarding the name and location of the database
(iv) information regarding the purpose of processing personal data in the database
(v) information regarding the content of the personal data
(vi) information on third parties to whom the personal data is to be transferred
(vii) information regarding cross-border transfer of personal data
(viii) information regarding other administrators of the database and
(ix) a commitment to protect personal data.

Failure to include the above information in the notice serves as grounds for the supervisory authority to reject registration of the database.

The supervisory authority must register the database within thirty business days of the date of submission of the notice. However, this term is currently not being met by the Agency due to certain objective reasons. According to the Agency, it has received over two million applications for registration of databases and it simply does not have the capacity to process all of them. Therefore, in practice, business entities have to wait about 3-4 months for their submissions to be at least officially accepted by the state officials. Under Ukrainian law, personal data can be processed once a personal database is registered. At the same time, the law does not provide for liability for processing personal data after the database registration documents have been submitted. The law provides for liability for non-registration of personal databases in case it is required.

Under the Data Protection Act, a data controller will obtain a document confirming the registration of the database in the Register. The data controller must then inform the supervisory authority of any further changes to the information contained in the database within ten business days of when such change occurs.

The Data Protection Registry is available at the following link: rbpd.informjust.ua/

Starting 01 January 2014, the requirement to register personal databases will be cancelled and replaced with a duty to notify the Ombudsman of the processing of personal data that constitutes a special risk to the rights and freedoms of the data subjects ('High Risk Data'). The notification must be submitted by the data controller within thirty working days of when it starts processing the data. Types of data classified as High Risk Data and the data controllers bound by the notification requirement are yet to be decided by the Ombudsman. At the date of this Guide, it remains unclear whether previously registered databases will need to be notified to the Ombudsman.

17. Are there any exemptions from the registration obligation?

Yes, there are to types of database that are exempt from the registration duty. These are databases containing personal information of (i) employees or (ii) members of non-governmental and religious organisations, trade unions and/or political parties

Moreover, the following are specially exempt from the ambit of the Data Protection Law in the creation of databases and the processing of their personal data in such databases:

(i) individuals, if an individual performs activity solely for personal (non-professional) and household needs and
(ii) creative professionals (artists, writers, etc.), including journalists, if they perform their official or professional duties provided only 'a balance between a right to privacy and a right to self-expression' is maintained.

Therefore, the registration obligation does not apply in these cases.

Effective as of 01 January 2014, the requirement to register the databases will be cancelled.

18. Are there any specific notification obligations?

Under the Data Protection Law, a controller must notify the Agency or, effective as of 01 January 2014, the Ombudsman, of any change of the data specified in the registration notice within ten business days of the date such change took place.

19. Does the relevant person have the right to access, rectify, remove or block their personal data?

Under the Data Protection Act the relevant person has, inter alia, the following rights with respect to his/her personal data processing:

(i) access his/her own personal data contained in the database
(ii) submit a justified request to rectify or delete personal data by any data controller or processor, if such data is processed illegally or is inaccurate in any respect
(iii) submit an objection to the processing of his/her personal data
(iv) set out certain restrictions/reservations with respect to any element of his/her personal data processing
(v) obtain information on the terms of third parties' access to his/her personal data, including information about third parties to whom his/her personal data are transferred
(vi) revoke his/her consent to the personal data processing.

20. What are the sanctions for data controllers that infringe the obligations (i.e. fines, criminal liability, civil liability, or any other)?

Criminal and administrative liability for failing to comply with the data protection legislation is set out by the Ukrainian Law on Amendments to Certain Legislative Acts of Ukraine to Increase Liability for Violation of Personal Data Protection Law (the 'Liability Law').

Under the Liability Law, financial sanctions are established for incompliance with certain rules. For example, if the data controller evades state registration of databases containing personal data, or fails to inform the relevant person about his/her rights in connection with personal data processing, or is not in compliance with the established order of personal data protection, the data controller could face a fine in an amount up to UAH 17,000 (ca. €1,700).

Illegal collection, storage or dissemination of personal data could lead to criminal liability, such as high fines or even imprisonment for up to five years.

Moreover, if a breach of legal requirements concerning personal data protection caused any damage to the relevant person, the latter may seek compensation for such damage in court.

Key contacts

Bulgaria

CMS Cameron McKenna LLP - Bulgaria Branch
Landmark Centre
14 Tzar Osvoboditel Blvd.
1000 Sofia, Bulgaria
T +359 2 92199 10
F +359 2 92199 19

David Butts
Managing Partner
T +359 2 92199 48
E david.butts@cms-cmck.com

Angelika Dimitrova
Associate
T +359 2 92348 51
E angelika.dimitrova@cms-cmck.com

Czech Republic

CMS Cameron McKenna v.o.s.
Palladium, Na Poříčí 1079 / 3a
110 00 Prague 1, Czech Republic
T +420 296 798 111
F +420 221 098 000

Tomáš Matějovský
Partner
T +420 296 798 852
E tomas.matejovsky@cms-cmck.com

Jakub Tomšej
Associate
T +420 296 798 808
E jakub.tomsej@cms-cmck.com

Hungary

CMS Cameron McKenna LLP
Ormai és Társai
YBL Palace
Károlyi utca 12
1053 Budapest, Hungary
T +36 1 48348 00
F +36 1 48348 01

Dóra Petrányi
Partner
T +36 1 48348 20
E dora.petranyi@cms-cmck.com

Márton Domokos
Senior Associate
T +36 1 48348 24
E marton.domokos@cms-cmck.com

Poland

CMS Cameron McKenna
Dariusz Greszta Spółka Komandytowa
Warsaw Financial Centre
Ul. Emilii Plater 53
00-113 Warsaw, Poland
T +48 22 520 5555
F +48 22 520 5556

Tomasz Koryzma
Partner
T +48 22 520 8479
E tomasz.koryzma@cms-cmck.com

Marcin Lewoszewski
Associate
T +48 22 520 5525
E marcin.lewoszewski@cms-cmck.com

Romania

CMS Cameron McKenna SCA
S-Park 11–15, Tipografilor Street
B3–B4, 4th Floor
District 1, 013714 Bucharest
T +40 21 4073 800
F +40 21 4073 900

Gabriel Sidere
Managing Partner
T +40 21 4073 813
E gabriel.sidere@cms-cmck.com

Marius Petroiu
Senior Associate
T +40 21 4073 889
E marius.petroiu@cms-cmck.com

Russia

CMS Hasche Sigle
CMS, Russia
Gogolevsky Boulevard, 11
119019 Moscow, Russia
T +7 495 786 4000
F +7 495 786 4001

Leonid Zubarev
Partner
T +7 495 786 4000
E leonid.zubarev@cmslegal.ru

Elena Baryshnikova
Associate
T +7 495 786 4000
E elena.baryshnikova@cmslegal.ru

Slovakia

Ružička Csekes s.r.o.
in association with members of CMS
Vysoká 2/B
811 06 Bratislava , Slovakia
T +421 2 3233 3444
F +421 2 3233 3443

Adriana Kováčiková
Partner
T +421 2 3233 3432
E adriana.kovacikova@rc-cms.sk

Hana Supeková
Associate
T +421 2 3233 3421
E hana.supekova@rc-cms.sk

Ukraine

CMS Cameron McKenna LLC
6th Floor, 38 Volodymyrska Street
01030 Kyiv, Ukraine
T +380 44 39133 77
F +380 44 39133 88

Olexander Martinenko
Partner
T +380 44 39177 04
E olexander.martinenko@cms-cmck.com

Olga Belyakova
Senior Associate
T +380 44 39177 27
E olga.belyakova@cms-cmck.com

Nataliya Nakonechna
Senior Associate
T +380 44 39177 29
E nataliya.nakonechna@cms-cmck.com

It fields a team of truly specialised lawyers who provide quick, strategic and commercially sound advice.

Chambers and Partners 2013

Law-Now™

CMS Cameron McKenna's free online information service

Receive expert commentary and analysis on key legal issues affecting your business. Register for free email alerts and access the full Law-Now archive at **www.law-now.com**

CMS Cameron McKenna LLP
Mitre House
160 Aldersgate Street
London EC1A 4DD

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

1306-000059-6