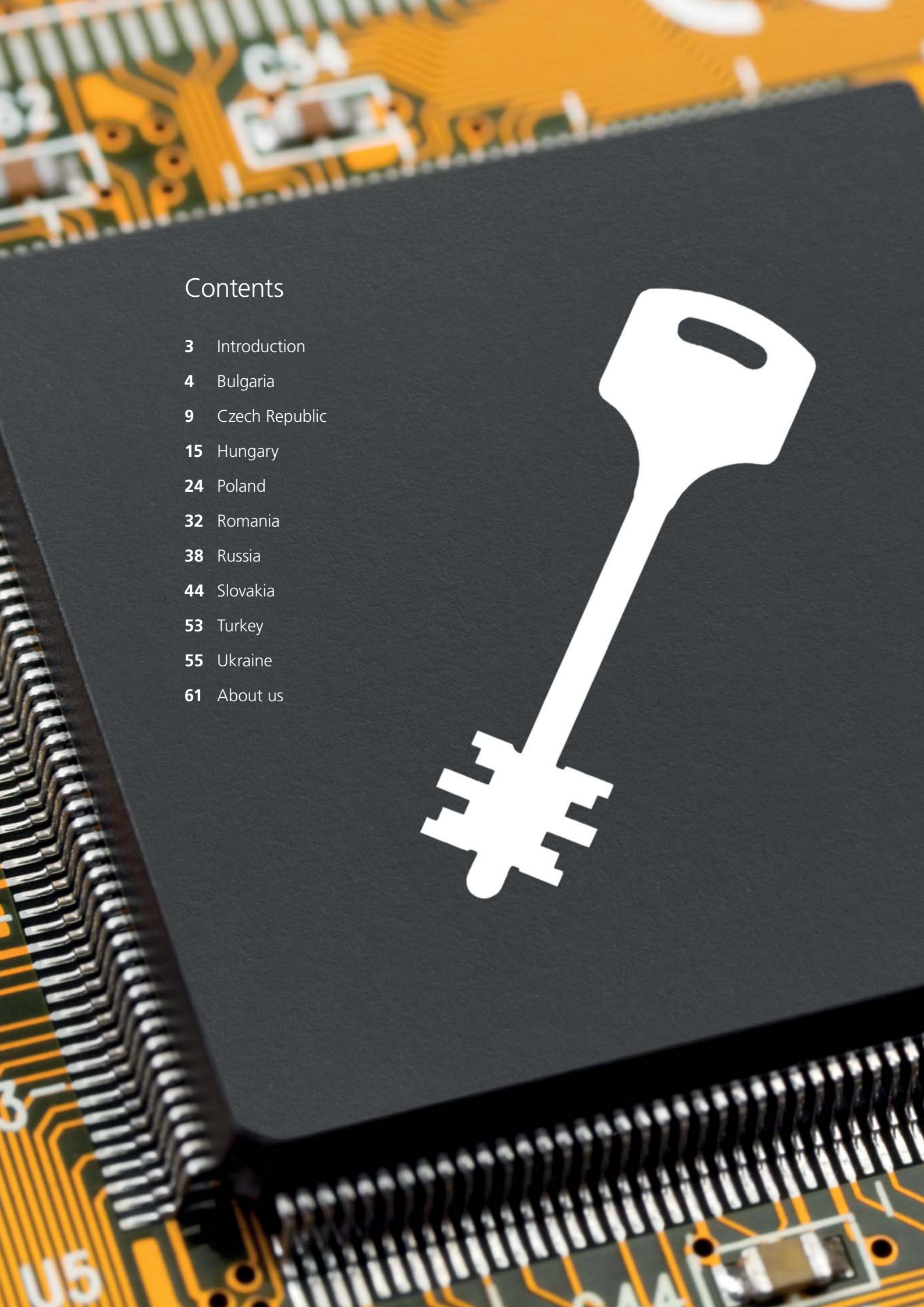
Your World First

CMS Law.Tax

Your guide to data protection in CEE

2015 - 2016

Contents



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 CEE with the aim of providing an overview of the various national personal data protection frameworks that exist in the region. 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, Czech Republic, Hungary, Poland, Romania, Russian Federation, Slovakia, Turkey and Ukraine.

CMS 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 December 2015.

CMS' 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 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
Head of CEE Commercial Practice
T +48 22 520 5528
E iain.batty@cms-cmck.com

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

Bulgaria

1. Applicable law

The Bulgarian Data Protection Act dated 4 January 2002, as amended ('Data Protection Act') implements Directive 95/46/EC into Bulgarian law.

The Data Protection Act defines personal data and data processing, regulates consent rules, data transfers, 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 circumstances of the case.

The Data Protection Act applies to the processing of personal data where the data controller:

— is established in the territory of the Republic of Bulgaria and processes personal data in regard to its activity

— is not established in the territory of the Republic of Bulgaria but must apply the Data Protection Act by virtue of international public law or

— 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. The data protection authority (DPA)

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. Appointment of internal data protection officers

The appointment of an internal data protection officer is not required by the Data Protection Act. Any such appointment is voluntary.

4. Internal privacy policies and external privacy notices

In our experience most international companies active on the market have internal policies for personal data protection as well as mandatory-required internal rules for the protection of databases. The Data Protection Act expressly provides that industry-specific codes of ethics applicable to data controllers may also be prepared.

5. 'Personal data' and 'sensitive 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 to be 'personal data'. Thus qualification of data as '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') the processing of which is generally prohibited, unless for e.g. with the explicit consent of the data subject and where the applicable laws permit it. Such sensitive personal data would be those 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. The minimum age for collection of personal data

There is no explicit requirement under the Data Protection Act regarding the minimum age for the collection of personal data. The general principle which applies is that: (i) people under the age of 14 are minors with no capability to perform legal acts; (ii) people between 14-18 years of age have limited capability; and (iii) people above 18 years of age are fully capable of performing legal acts.

7. Consent requirements (general, special categories and marketing)

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 the consent of data subjects even when it is not mandatory. Consent under the Data Protection Act means 'any freely given, specific and informed statement of volition by which the individual to whom personal data relate signifies unambiguously his or her consent to such data being processed.' There is no particular form required, but written form is strongly advisable.

8. Processing without consent

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

— compliance with a legal obligation applicable to the data controller

— the fulfilment of obligations under an agreement to which the individual to whom such data relates is a party, as well as for any activities initiated by the same individual prior to the conclusion of the agreement

— the protection of the life and health of the individual to whom the data relates

— the performance of a task carried out in the public interest

— the exercise of an official authority vested by law in the data controller or in a third party to whom the data is disclosed

— the realisation of the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests of the individual to whom the data relates.

In addition, personal data may be processed exclusively for the purposes of journalism, literary or artistic expression, to the extent that this does not violate the data subject's right to privacy.

9. Data transfers

The transfer of data to an EU/EEA member state is treated as being the same as the transfer of data within the territory of Bulgaria - it shall be done freely, subject to compliance with the requirements of the Data Protection Act.

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 (or the EC) unless EC Model Clauses are used.

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

— the relevant person has provided express consent to the transfer, or

— the transfer is required for the fulfilment of obligations under an agreement between the data controller and the data subject as well as any activities initiated by the latter prior to the conclusion of the agreement or 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, or

— 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, or

— the data source is a public register, the access to which is performed as provided for under applicable law, or

— the data transfer is performed only for the purposes of journalism, literary or artistic expression, to the extent that this does not violate the data subject's right to privacy.

Finally, personal data may be transferred to a third country after an authorisation from the DPA, if the data controllers in both countries (the data exporter and the data importer) provide sufficient guarantees for the data protection.

In practice, the DPA adopts quite a restrictive approach to the transfer of personal data. The controller's intention to transfer personal data within the EU/EEA or to third countries must be notified to the DPA as part of the controller's registration obligations (accordingly the changes to such transfer must also be notified to the

DPA). It is advisable to make a notification of any data transfer to a third country. The notification has just informative functions. Authorisation is required in the cases provided for by the Data Protection Act (i.e. when it is necessary for the DPA to evaluate the adequacy of the data protection in the third country; or if the data exporter and the data imported have opted to provide sufficient guarantees for the data protection).

10. Intra-group transfers

The Data Protection Act does not provide for specific regulations relating to intra-group transfers. A group company is regarded as a third party, and, as above, would either (a) need to independently satisfy the legal requirements for data processing, or (b) the data privacy consent provided to the 'original' data controller must contain consent to the processing/transfer between the group companies, and/or (c) the relevant companies should enter into a written data transfer agreement based on EC Model Clauses in order to ensure compliance with the data transfer obligations stated above (see also Section 9 on Data Transfers). BCRs are also applicable to intra-group data transfers although they are not expressly listed in the Data Protection Act or the Directive 95/46/EC.

11. Mandatory data protection information

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 the data processing the relevant person must be given clear and detailed information on all circumstances relating to the data processing, including:

— the identity of the controller and its representative, if any

— the purposes of the data processing

— the recipients or categories of the recipients to whom the data may be revealed

— whether providing the data is mandatory or voluntary, as well as the possible consequences of failing to provide the data, and

— the existence of the data subject's 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:

— 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

— communication in an intelligible form of the data undergoing processing and of any available information as to its source, and

— knowledge of the logic involved in any automatic processing of data concerning the person at least in the case of automated decisions.

12. Notice & consent language requirements

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.

13. Appointment of data processors

Controllers may process data themselves or assign it to data processors. When assigning the data processing is required for organisational reasons, processing may be assigned to more than one data processor and their specific tasks must be 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 the 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 omission of 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 only process such data on the instructions from the controller, unless otherwise provided for by the law.

14. Data retention

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 (this notification is not related to transfers to non-EU countries. It is mandatory in the case of transfers to another controller for identical purposes of processing and if the transfer is provided for by law).

Storage is permitted – if the purpose of the processing has been achieved – only if provided for by law (e.g. storage as anonymous data for historical, scientific or statistical purpose) and subject to a notification to the DPA. The DPA may prohibit the storage of data if in its option the controller has not provided enough guarantees for storing the data as anonymous.

15. 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, unauthorized disclosure or access, in particular where processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Specific security measures should be undertaken in the case of transfers 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 minimum level of technical and organisational measures required is subject to a specific ordinance issued by the DPA (*'Ordinance No. 1 dated 30 January 2013 for the minimum level of technical and organisational measures and permissible types of protection of personal data'*).

16. Other specific obligations

There are no other specific obligations listed in the Data Protection Act.

17. 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 (unless the controller has applied for processing of sensitive data, in which case the preliminary inspection would continue for two months, during which period the controller is not allowed to process such data).

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

18. Exemptions from the registration

Registration is not required if:

— 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, or

— 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.

19. 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.

20. Data protection rights and remedies

The data controller 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. Such application shall be considered by the controller within 14-days or 30-days period in more complex cases, and free of charge.

A data subject also has the right:

— 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

— to object to the processing of his or her personal data for the purposes of direct marketing, and

— 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.

21. Sanctions for non-compliance

(A) Administrative remedies and other sanctions

The data subject, whose rights are infringed, may file a complaint with the DPA within one year of the date when he/she has become aware of such infringement but not later than five years of the date when such infringement has taken place. In such cases the DPA shall issue a decision within 30 days and may:

— provide mandatory recommendations that must be immediately observed by the data controller, or

— set a time limit for the infringer to remedy the consequences of the infringement, or

— impose a fine of up to BGN 100,000 (approximately EUR 50,000) and to double this amount in the case of recurring breaches.

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.

The DPA's decision may be appealed before the competent administrative court within 14 days of its receipt.

(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 and claim damages.

(C) Criminal law issues

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 (e.g. if passwords or codes for access to a computer system or computer data have been disclosed and this has resulted in an illegal disclosure of personal data).

David Butts
Managing Partner
T +3592 921 99 48
E david.butts@cms-cmck.com

Angelika Dimitrova
Associate
T +3592 921 99 51
E angelika.dimitrova@cms-cmck.com

CMS Cameron McKenna LLP
- Bulgaria Branch
Landmark Centre
14 Tsar Osvoboditel Blvd.
Floor 1
Sofia - 1000
Bulgaria

T +3592 921 99 10
F +3592 921 99 19

Czech Republic

1. Applicable law

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 transfers, 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/uoouaspx?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. The data protection authority (DPA)

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. Appointment of internal data protection officers

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. Internal privacy policies and external privacy notices

In our experience, both internal and external privacy notices are good market practices that many companies observe.

5. 'Personal data' and 'sensitive 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 attitude, 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. The minimum age for collection of personal data

It is possible to process personal data of any persons irrespective of their age.

Where consent with the data processing is necessary, it must be examined whether a minor can grant such consent. A person becomes legally competent after having reached the age of 18, unless he/she was expressly declared legally competent by court at a lower age. Under the general principles, children under the age of 18 may only legally act where such act corresponds to their mental and moral maturity.

It is presumed that children under the age of 15 cannot grant a data processing consent and such consent must be sought from their parents. In case of minors who have reached 15 years of age but are not fully legally competent, it must be assessed on a case-by-case basis whether they possess a sufficient level of understanding to be able to grant the consent.

7. Consent requirements (general, special categories and marketing)

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 Section 8 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 data processing for the whole period of the processing. For this reason, it is in most cases recommended to obtain consent in writing.

8. Processing without consent

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

- if the processing is essential to comply with the controller's legal obligation (e.g. an employer processing the personal data of its employees to the necessary extent)
- 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
- 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
- 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
- if it is essential for the protection of the rights and legitimate interests of the controller, recipient or other person concerned. However, such data processing may not be in contradiction with the right of the relevant person to the protection of his/her private and personal life
- 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
- 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:

- 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
- 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
- if the processing is necessary due to the obligations and rights of the data controller in the fields of labour law and employment
- 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
- 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
- if the processing concerns personal data published by the relevant person
- if the processing is necessary to secure and exercise legal claims
- if they are processed exclusively for archival purposes
- 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.

9. Data transfers

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.

10. Intra-group transfers

The Data Protection Act does not acknowledge holding companies as a specific subject of regulation; therefore no different regulation applies.

11. Mandatory data protection information

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), and if

— 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

— the data processing is imposed on him/her by a special act or such data are necessary to exercise the rights and obligations ensuing from special acts

— it is processing exclusively lawfully published personal data (e.g. from the Commercial Register)

— (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).

12. Notice & consent language requirements

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 a 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.

13. Appointment of data processors

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 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.

14. Data retention

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 documents. As an example, a longer retention period may apply to documents relating to the 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.

15. 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:

— the provision of instructions for data processing by persons who have immediate access to the personal data

— the prevention of unauthorised people from accessing personal data and the means for their processing

— the prevention of unauthorised reading, creating, copying, transferring, modifying or deleting of records containing personal data, and

— 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. EUR 200,000) can be imposed.

16. 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.

17. 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:

— the identification data of the controller

— the purposes of processing

— the categories of the persons affected and of the personal data pertaining to these subjects

— the sources of personal data

— a description of how the personal data will be processed

— the location or locations of data processing

— the recipient or category of recipients

— the anticipated personal data transfers to other countries

— 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.

18. Exemptions from the registration

Registration in the Data Protection Registry is not necessary if:

— 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), or

— 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

— 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).

19. Specific notification obligations

There is a specific notification obligation in the case of data transfer to third countries (please refer to Section 9 above).

20. Data protection rights and remedies

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/her personal data, the data controller must provide him/her with this information without undue delay.

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

— the purpose of processing the personal data

— the personal data or categories of personal data that are subject to processing including all available information on their source

— 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

— 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 controllers 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:

— ask the controller or processor for an explanation

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

21. Sanctions for non-compliance

(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 a 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. EUR 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. EUR 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 breach of data protection regarding personal data collected by public authorities when carrying out their statutory duties, or

— a breach of the duty of mandatory confidentiality, imposed or acknowledged by the state (e.g. attorneys-at-law, doctors, priests, etc.)

If such a 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.

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

CMS Cameron McKenna v.o.s.
Palladium, Na Poříčí 1079/3a
Prague - 110 00
Czech Republic

T +420 296 798 111
F +420 296 798 000

Hungary

1. Applicable law

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: http://www.naih.hu/act-cxii-of-2011---privacy-act--.html.

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.

Hungarian authorities also tend to interpret the scope of the Data Protection Act extensively: in the so-called 'Weltimmo case', a company established in Slovakia was fined because it operated a website containing advertisements of properties located in Hungary and collected personal data of Hungarian buyers and sellers. In such case, the Court of Justice of the European Union (CJEU) has ruled that the data protection legislation of a Member State may apply to a data controller registered in another Member State if, through stable arrangements in the territory of that Member State, the data controller exercises a real and effective activity, however minimal, in the context of processing personal data.

2. The data protection authority (DPA)

Hungarian Authority for Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság – 'NAIH'*). Its website can be found at www.naih.hu/.

3. Appointment of internal data protection officers

The following controllers and processors must appoint or engage an internal data protection 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:

— companies processing nationwide jurisdictional, employment and criminal records

— financial institutions

— electronic communications service providers and public utility services providers.

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

It is advisable for data protection officers to register themselves with the NAIH. The so-called 'conference of internal data protection officers' provides for professional liaison between internal data protection officers and the NAIH 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 NAIH 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 protection officers' registry kept by the NAIH.

The internal data protection officer shall:

— participate and assist in the decision-making process with regard to data processing and enforcing the rights of data subjects

— monitor compliance with the Data Protection Act and other regulations on data processing as well as with the provisions of internal data protection and data security regulations and other data security requirements

— investigate complaints and, if he/she detects any unauthorised data processing, calls on the controller or processor in question to cease such operations

— prepare the internal data protection and data security rules

— maintain the internal data protection register(s) and

— arrange internal data protection training sessions.

4. 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, electronic communications service providers, public opinion survey makers, market research and direct marketing organisations. 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.

NAIH expects that controllers performing more complex data processing, or having bigger organisations, should have a specific internal privacy policy, which describes for the employees performing data processing all the tasks and obligations during these activities.

If the controller has different departments, with more people having access to personal data in the organisation, the external privacy notice should include the processing terms of each department.

5. 'Personal data' and 'sensitive 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 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: (i) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, and (ii) personal data concerning health, addictions, sex life, or criminal record.

The Data Protection Act only applies to information about individuals as opposed to legal entities.

6. The minimum age for collection of personal data

Hungarian law - Act V of 2013 on the Civil Code ('**Civil Code**') and the Data Protection Act - regulates the legal age as follows:

— Minors below 14 ('minors without legal capacity'). Their legal statements shall be, without the approval of their legal representatives, null and void; their parents shall proceed on their behalf.

— Minors above 14 who are not incompetent ('minors of limited capacity') shall, without the participation of their parents, be entitled to (i) conclude contracts of minor importance aimed at satisfying their everyday needs; or (ii) to conclude contracts that only offer advantages.

— The privacy consent of minors over the age of 16 shall be considered valid without the permission or subsequent approval of their parents.

Controllers need to decide on a case-by-case basis whether a proposed processing may be considered as (i) contract of minor importance aimed at satisfying everyday needs; or (ii) contract that only offer advantages. According to the findings of the NAIH, in such cases, the privacy consent does not require the approval of the parents. However, this shall be applied reasonably because the overlap between the laws is rarely tested yet by courts or NAIH. In a case the NAIH imposed HUF 100,000 (approx. EUR 330) on a company because it failed to inform minors below 16 that their data privacy consent requires the approval of their legal representative. In another case, HUF 450,000 (approx. EUR 1,500) fine was imposed because a company operating a dating website processed the personal data of children below 14. The NAIH recommends that (i) controllers need to inform minors between 13 and 14 that their legal statements shall be, without the approval of their legal representatives, null and void; and (ii) controllers need to provide a .pdf template at their website for the parental consent, which can be sent back via fax or post, or a toll-free number for parents to call and consent to the processing of the data of their children.

7. Consent requirements (general, special categories and marketing)

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). If the consent is provided electronically and the relevant person is identifiable unambiguously, the NAIH considers it as being in writing. The controller must always be in the position to prove that consent has been provided properly and lawfully, so proper archiving is advisable. The NAIH also pointed out that the consent is not free and express if the 'yes' checkbox is ticked in advance by default and does not require any action from the user besides proceeding with the registration.

As regards advertising, Hungary operates an 'opt-in' regime. Advertisements may be sent to private individual end-users in the territory of Hungary by way through e-mail or similar electronic channels only upon the express prior consent of the addressee. Consents for individual marketing activities shall contain the name, place and date of birth (if the marketing can be targeted only for people above a certain age) and the list of the personal data of the consumer which are processed in relation to the marketing. In addition, the consent shall contain that it is provided voluntarily, on the basis of adequate information provided to the consumer. In all cases, end-users shall be expressly informed in all individual marketing communications of the opportunity to freely opt-out from the communications and the relevant contact details (postal and email address) where they can do so. Such statement is usually inserted in the footer of the marketing communications. If the consent is provided in a contract or general terms, it shall be provided separately from the main text (e.g. via the acceptance of a separate consent box) and it cannot be a precondition to the contracting or obtaining a service, such as a webshop. If the advertiser offers added value, provided that the addressee consents to receiving DM messages, no separate consent box may be needed – for example, if the addressee is provided with the opportunity to participate in a game or use free email services. If the private individual addressee is an employee of a legal entity, and the advertiser obtained the contact details lawfully (e.g. via the company's website or public sources), and the advertisement is targeted to the company, the DM message can be lawful. In all cases, an internal register shall be kept of the persons who provided opt-in consent for individual marketing activities which shall include the (i) name; and (ii) the place and date of birth of the addressee.

8. Processing without consent

Personal data can be processed even if obtaining the consent proves impossible or involves a disproportionate cost and if the processing is necessary for:

— compliance with a legal obligation applicable to the controller, or

— the purpose of legitimate interests of the controller or third parties and such necessity is proportionate to the restriction of privacy.

In the above cases data may also be processed if the relevant person withdraws his/her consent (which can be done at any time under the law). This 'legitimate interest' exception may be applied, for example, in cases where 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 processing, if this can unreasonably delay or prevent the achievement of the desired goal. According to the NAIH, the term 'legitimate interest' cover 'lawful and fair business interests'.

To rely on the 'legitimate interest basis', controllers shall perform a so-called 'balance of interests' test, where they shall identify the legal interest of the controller, the data subject and the underlying fundamental right, and whether the personal data may be processed as the result of the balancing. Data subjects should be informed on the result of the test (why the legitimate interest is more important than the underlying privacy rights and interest of the data subject). Data subjects should be informed of the data protection measures undertaken with a view to the lack of consent, and the possibility to object to the processing.

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 cost') cannot be derived from Article 7 of Directive 95/46/EC either. (Directive 95/46/EC enables that that personal data may be processed if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.) The publicly available guidance of the NAIH 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, controllers may apply its provisions directly; however, this must be assessed carefully, and always on a case-by-case basis.

9. Data transfers

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.

Controllers or processors may transfer personal data to controllers or processors in third countries if

— it is expressly approved by the relevant person, or

— the conditions of 'legitimate interest' are met (see question No. 8) 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, or an 'EU Model Clause' is concluded in respect of the data transfer, or Binding Corporate Rules for International Data Transfers (BCRs) are adopted. EU Model Clauses may not be filed with the NAIH. Since 1 January 2012, entering into other individual data transfer agreements is not considered as providing 'adequate protection' anymore.

10. Intra-group transfers

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

11. Mandatory data protection information

Before the commencement of data processing the relevant person must be given clear and detailed information of all circumstances in relation to the processing, including:

— the voluntary or mandatory nature of the processing

— the specific list of the data processed

— the specific purpose and legal basis for processing (with the underlying legal provision)

— the identification of the controller(s) and the processor(s) (name, address, telephone, regularly used email, website where the privacy notices and policies are available)

— the duration of the processing (by reference to the relevant legal provision, if possible)

— who can access the data

— list of the data transferees, together with the data transferred and the purpose of each transfer, the capacity of the transferee (controller / processor), and the terms of the data processing performed by them (e.g. a link to their data protection policy)

— in case of data processing, the list of personal data that the data processor can access, the duration of this activity and the exact operations of the processor with such data

— if there is any data transfer to a third country and if no 'adequate level' of protection is given to personal data in such country

— the rights and remedies of the relevant persons (information, rectification, blocking, deletion, objection and appealing to the NAIH or court, contact details of the data controller)

— if the controller will not be able to delete the data despite the relevant person's request because the data are needed for legitimate purposes

— brief and clear description of data security measures

— prior information if there is automated decision making

— the registration number (if any) of data processing at the NAIH.

The practice of the NAIH provides that it is advisable to avoid reference to 'potential' data processing (e.g. it is recommended to use the term 'will transfer data' instead of 'may transfer data'). According to the NAIH, in case of multiple data transfers with different processing purposes (e.g. DM messages from transferees in different industries) users shall provide their consent to each type of transfer separately. (Also providing a 'select-all' checkbox would be acceptable.)

Privacy notices shall be continuously accessible on the opening page of controller's website and also during the most important steps of the processing (e.g. before and in the course of a registration process). In case of technical limits (like the size of a ticket) at least the processing and the controller shall be indicated with a link to the privacy notice. It is possible to insert the privacy notice into general terms and conditions but it shall be separated clearly.

12. Notice & consent language requirements

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 controller must prove that the relevant person understood the language of the notice and consent, so bilingual documents are recommended. If the processing covers the personal data of foreign people (e.g. a guest book or an international tender), the privacy notice must be available in English. If needed, the controller should make it possible for disabled people to get to know the privacy notice without any obstacles.

13. Appointment of data processors

'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.

The Data Protection Act does not define the mandatory contents of such agreements. According to the practice of the NAIH, the following issues should be regulated in data processing agreements:

— Exactly defining the legal relationship of the parties and the relevant powers.

— Specifying the actual activities carried out with personal data / who has what tasks in relation to the data in the course of the cooperation? (In the opinion of the NAIH it is not sufficient to have a too general agreement between the parties in place that it is the performance of the tasks of 'data controller' or 'data processor'.).

— What could be the technical operations, organisational issues not requiring any decision on the merits which the data processor is entitled to carry out on its own?

— What could be the decisions on the merits in which the processor is not entitled to decide on its own in the absence of any instruction or specification from the controller?

— Providing for whether the processor is entitled to act towards end-users in its own name? If yes, it should be expressly communicated to data subjects that the processor acts individually.

— Possibility for security audits and the formal requirements of the related documentation (origin, purpose of preparation, defining liability and tasks in the event of remedying shortcomings, etc.).

— Detailed cooperation obligation especially in the event of data security incidents or data theft (e.g. crisis management, remediation, prevention of the occurrence of further losses, defining exact deadlines).

— Data processing after the agreement ends: selection and deletion of data which does not need to be used/is not permitted to be used for further purposes (e.g. marketing).

— 'Surviving obligations' after the termination of the agreement.

— In case of data processing regarding promotions, stipulating that the promotional participation rules should be approved in advance if it is prepared by a third party.

Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data (e.g. competitors).

14. Data retention

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 authorized 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. Usually, employment-related data (e.g. internal correspondence) can be kept for 3 years, data with civil law nature (e.g. contract data, information on commitments) can be kept for 5 years, and if the document is relevant for accounting purposes (e.g. certificate of performance or payment), the retention period is 8 years.

15. 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 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). In determining the measures to ensure security of processing, data controllers and processors shall proceed taking into account the latest technical development and the state of the art of their implementation. Controllers and processors must simply choose the processing alternative that ensures a higher level of protection for data, unless this causes disproportionate difficulties.

The NAIH'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 NAIH 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 trainings and subsequent verification of compliance are also recommended. 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. It is also advisable to introduce encryption, and access verification measures.

In line with the amended Directive 2002/58/EC, electronic communications service providers have mandatory data security breach notification obligations. There are no mandatory data security breach notification obligations in other sectors. However, controllers shall keep an internal register of data security breaches ('Internal Data Security Breach Register'). Such Internal Data Security Breach Register shall contain the data affected, the scope and number of the people affected, the date, the circumstances, the effects of the breach, the measures taken to eliminate the breach, and any other data which data protection laws require the processing of. Electronic communications service providers can fulfil the above obligation by keeping the specific internal register required by electronic communications laws. The Internal Data Security Breach Register shall also cover breaches by data processors.

16. Other specific obligations

An internal data transfer registry ('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 processing.

17. Registration obligations at the DPA

Controllers must register with the NAIH in the Data Protection Registry (in Hungarian: *'Adatvédelmi Nyilvántartás'*) prior to carrying out any data processing. The registration procedure requires the completion of the NAIH'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 processing can commence only when the registration is made. The NAIH makes the registration within eight days; if it fails to do so, the processing can commence. Upon registration, the controller receives a registration number, to be indicated in all 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 NAIH within eight days of the effective date of the change. Registrations are made per processing purpose.

18. Exemptions from the registration

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

— concerning data of employees, members, kindergarten, students, dormitory services, or customers

— carried out in accordance with the internal rules of the church or other religious congregation or organisation

— 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

— which involves information concerning the provision of social and other benefits to the relevant person

— 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

— 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

— which involves the data of a media content provider, which are used solely for its own information activities

— if it serves the purposes of scientific research, and if the data is not made available to the public or

— which involves documents deposited in archive.

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 party controllers. Establishment of a database or data collection for future purposes is not exempt from the registration.

Employee data processing is exempted from the registration obligation if the data processing does not go beyond purposes which are necessary to the day-to-day management of employee data (e.g. administration, payroll). Any other type of processing (e.g. e-learning, operation of whistleblowing systems) shall be registered.

19. Specific notification obligations

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

— Financial institutions, public utility companies and electronic telecommunications service providers must register with the NAIH prior to carrying out any processing activities in relation to their customers.

— The NAIH 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.

— Controllers requesting or using name and address information for the purpose of establishing contact for scientific research, public opinion survey, market research and direct marketing reasons, prior to commencing the activities, shall report all data processing operations to the NAIH.

20. Data protection rights and remedies

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 processing, and – if the personal data of the relevant person is transferred to third parties – the legal basis and the recipients. The data controller 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 NAIH must be notified of refused information requests for a given year by 31 January of the next year.

Rectification

Controllers must rectify all incorrect personal data.

Deletion

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

— processed unlawfully

— so requested by the relevant person

— it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by law

— the purpose of processing no longer exists or the legal time limit for retention has expired

— so instructed by court order or by the NAIH.

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:

— 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

— if personal data are used or disclosed for the purposes of direct marketing, public opinion polling or scientific research, and

— in all other cases prescribed by law.

In the event of an objection, the 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 NAIH or to court

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

21. Sanctions for non-compliance

(A) Administrative remedies and other sanctions

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

— order the rectification of any personal data that is deemed inaccurate

— order the blocking, erasure or destruction of personal data processed unlawfully

— prohibit the unlawful processing

— prohibit the cross-border transmission or disclosure of data

— order the provision of an information to the relevant person, if it was refused by the controller unlawfully

— impose a fine of between HUF 100,000 (approx. EUR 320) and HUF 20,000,000 (approx. EUR 64,500), and

— 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 NAIH 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. According to the NAIH, it can be a mitigating factor if the controller is cooperating during the investigation and appropriately amends its privacy policy already in the course of the investigation. When determining the amount of the fine, the NAIH may consider the position of the company at the market and the income indicated in its annual financial statements. The NAIH may also determine the amount of the fine with a view to 'general prevention', i.e. as a warning to other companies to comply with the laws.

In particular cases, the NAIH may advise the controller to seek new data privacy consent from the relevant people, in line with its privacy policy amended with a view to the NAIH's findings. The controller should delete the data of those people who do not repeat their consent.

The Hungarian Consumer Protection Authority, the National Media and Infocommunications Authority ('NMHH') may impose a fine up to HUF 500,000 (approx. EUR 1,600) in case the rules on unsolicited communications are violated.

(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. The court may require the controller to reimburse damages or provide restitution (in Hungarian: 'sérelemdíj') for any non-pecuniary damage. In case of restitution, apart from the fact of the infringement, no other damages have to be proved. The court shall determine the amount of restitution in one sum, taking into account the gravity of the infringement, whether it was committed on one or more occasions, the degree of responsibility, the impact of the infringement upon the aggrieved party and its environment.

(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.

Dóra Petrányi
Partner
T +36 1 483 4820
E dora.petranyi@cms-cmck.com

Márton Domokos
Senior Counsel
T +36 1 483 4824
E marton.domokos@cms-cmck.com

CMS Cameron McKenna LLP
Hungarian Office
YBL Palace
Károlyi utca 12
Budapest - 1053
Hungary

T +36 1 483 4800
F +36 1 483 4801

Poland

1. Applicable law

Directive 95/46/EC has been implemented by the Polish Act of 29 August 1997 on the Protection of Personal Data Act (unified text – Journal of Laws 2014, item 1182, with amendments) ('Data Protection Act' or 'Act').

The Data Protection Act defines personal data, including sensitive data. The Act determines the principles of data processing and the rights of individuals (so-called data subjects) whose personal data is or can be processed as a part of a data filing system.

The Data Protection Act was amended by the Act on the facilitation of conducting business activity dated 7 November 2014[1] ('Amendment') which came into force on 1 January 2015. The amended Data Protection Act is available at the following link: www.giodo.gov.pl/144/id_art/171/j/en/.

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 shall 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.

More specific regulations concerning data processing in Poland are:

— the Regulation of 11 December 2008 on the template for notifying the General Inspector for Personal Data Protection of a data filing system (database)

— the Regulation of 29 April 2004 on documentation for processing personal data, and technical and organisational requirements for devices and computer systems used for processing personal data.

Moreover, there are three newly adopted Regulations, which are going to be discussed along with the updated rules of the appointment and duties of the Data Privacy Officer.

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

— the Insurance Activity Act 2003

— the Banking Law Act 1997

— the Labour Code Act 1974

— the Press Law Act 1984.

2. The data protection authority (DPA)

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

3. Appointment of internal data protection officers

A data controller decides on the purposes and means of processing personal data.

Until 1 January 2015, the legal person, acted as a data controller was obliged to appoint Data Privacy Officer (ABI). Under the amended regime, it is no longer mandatory to appoint a Data Privacy Officer, irrespectively whether the data controller is a legal or natural person.

As a consequence of the Amendment, a data controller who appoints a Data Privacy Officer will be exempt from the obligation to register its databases, unless it processes sensitive data. However, the Data Privacy Officer is obliged to ensure compliance with the provisions on personal data, by, for example, preparing scheduled and ad-hoc reports for the data controller and, if requested, for the GIODO. A Data Privacy Officer also needs to keep internal registers of the databases

[1]Journal of Laws 2014, item 1662

processed by the data controller. If a data controller does not decide to appoint a Data Privacy Officer, his/her tasks shall be performed by the data controller, including the obligation to notify and register the data filing system.

Three new Regulations regarding the Data Privacy Officer came into force along with the amendment of the Data Protection Act, namely:

— *Regulation of 10 December 2014 on templates regarding the notification of the appointment and dismissal of the Data Privacy Officer*

— *Regulation of 11 May 2015 on the procedure and manner of ensuring compliance with the provisions of data protection law by the Data Privacy Officer*

— *Regulation of 11 May 2015 on the procedure and manner of conducting the Register of databases by the Data Privacy Officer.*

4. Internal privacy policies and external privacy notices

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 15 below.

There is no obligation to have an external privacy notice. However, if a company provides online 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 online 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 online service provider and its name and address, particular threats related to the use of such services, functionality of the software used by the online service provider and the possibility of discontinuing the services at any time.

5. 'Personal data' and 'sensitive 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: (i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, political party or trade-union membership, and (ii) personal data concerning health, genetic code, addictions and sexual orientation, or criminal record and (iii) personal data relating to criminal convictions, decisions on penalties, fines and other decisions issued in court or administrative proceedings.

6. The minimum age for collection of personal data

The Data Protection Act does not indicate the minimum age of data subjects. Thus, the general rules of Polish Civil Code ('Civil Code') are applicable.

Consequently, collecting data from persons who have not attained the age of thirteen (with no capacity for juridical acts) should require the consent of his/her

statutory representative. At the same time, it is crucial to stress, that the Civil Code allows persons incapable of juridical acts to enter into contract *generally concluded within petty, current matters of everyday life*, without the control of representatives, unless it results in a gross detriment to a person incapable of juridical acts.

The collection of personal data from data subjects with limited capacity for juridical act (age 13 – 18 years old) shall also require the consent or at least confirmation of a statutory representative.

There is a dispute in doctrine whether the statutory representative's control is indeed needed. At any time, however, such consent is required in case of processing sensitive data.

7. Consent requirements (general, special categories and marketing)

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. Electronic consent may be acceptable through an '*acceptance button*' or '*consent box*'. However, processing of sensitive data as well as the transferring data outside the European Economic Area requires written consent. According to Article 78 of the Civil Code, to comply with the written form, signing the printed document by wet signature is sufficient. Such written consent may be also made by electronic means with a secure electronic signature verified by a valid qualified certificate.

Under Polish law sending unsolicited commercial information by means of electronic communications (e.g. emails, messages via Internet communicator) is not allowed without the addressee's consent (spamming, Article 10 Sec. 1 of the Act on Provision of Services by Electronic Means). The same applies to contacting phone users, either by calling or sending an SMS for marketing purposes (Article 172 Sec. 1 of the Telecommunications Law). The consent has to be directly expressed ('opt-in' option) and cannot be implied from any other statements.

The processing data in marketing purposes does not require the data subject's consent when such marketing is considered the 'legitimate interest' of a data controller. However in that case the data subject can object to the processing of his/her data for marketing purposes or demand (in writing) the blocking of the processing of his/her data for marketing purposes due to data subject's particular situation.

8. Processing without 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.

9. Data transfers

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. 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.

The transfer of personal data to the third country may take place if the country of the destination ensures adequate level of personal data protection in its territory. Such adequacy shall be evaluated taking into account all circumstances concerning a data transfer operation, in particular the nature of the data, the purpose and duration of data processing, the country of origin and the country of final destination, legal provisions being in force in a given third country, as well as the security measures and professional rules applied in this country.

The above does not apply when the transfer is required by law or by the provisions of any ratified international agreement. The data controller can transfer the data to the third country provided that:

— the data subject has given his/her written consent

— the transfer is necessary for the performance of a contract between the data subject and the 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.

Until 1 January 2015 neither standard contractual clauses accepted by the EU Commission, nor binding corporate rules were recognised by the GIODO as a sufficient legal basis for transferring personal data internationally. Both instruments required authorisation from the GIODO. Under the amended Data Protection Act, the GIODO's authorisation is not required if the data controller ensures adequate safeguards for the protection of privacy and the rights and freedoms of the data subject, by executing:

— 'standard contractual clauses' approved by the European Commission in accordance with Art. 26 paragraph 4 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

or

— legally binding rules or policies of protection of personal data, also referred to as 'binding corporate rules' approved by the GIODO in accordance with the Polish data protection law. GIODO must approve binding corporate rules, adopted within a group of business entities, for the transfer of personal data by the data controller or data processor belonging to the same group to another controller or data processor located in a third country. Before approving binding corporate rules GIODO may consult the relevant data protection authorities of EEA countries on whose territory the entities belonging to the same capital group as the applicant are established, providing them with the necessary information. When issuing its decision, the regulator takes into account the results of the consultations with authorities from other EU countries, and if the binding corporate rules have been the subject of a decision of the data protection authority of another EEA country – may take this decision into consideration.

  According to the European Court of Justice ruling of 6 October 2015 - the Decision 2000/520 of the European Commission stating that the Safe Harbor-certified US companies provide adequate protection for personal data transferred to them from the EU, is invalid. Thus, the transfer of data from Poland to US companies which have completed the US-EU Safe Harbor adherence process requires the legal basis provided by the Polish law for such transfer, such as e.g. binding corporate rules authorised by GIODO.

10. Intra-group transfers

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.

11. Mandatory data protection information

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:

— the address of its seat and its full name, and if the controller is a natural person – its name and surname and address

— the purpose of data collection, and, in particular, about the data recipients or categories of recipients, if known on the date of collecting

— 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

— the right of the data subject to access his/her data and to rectify the data.

12. Notice & consent language requirements

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.

13. Appointment of data processors

A data controller may outsource 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.

14. Data retention

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.

15. Mandatory technical, organisational or security measures

In Poland, the rules for technical and organisational measures in relation to the 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 are 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 are 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.

16. 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.

17. Registration obligations at the DPA

A data controller is obliged to notify the GIODO about any database and to submit it for registration. A data filing system (database) includes any structured set of personal data which are accessible pursuant to specific criteria. 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 prior registration of the database with the GIODO. 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 2008 Regulation on the template for notifying the GIODO of a data filing system or online through the online registration service provided by the GIODO at the following address: egiodo.giodo.gov.pl/formular_step0.dhtml?c=0.6361029927790196. In the latter case, a notification transmitted electronically needs to be signed with the applicant's wet signature and sent by post or submitted to the GIODO's headquarters.

The notification itself should not include the content of the actual data, but should specify the following:

— that it is an application to enter the database into the GIODO's register of databases

— details concerning the entity running the database, and the legal grounds on which that person is authorised to run the database

— the purpose of the processing of the personal data

— a description of the categories of data subjects and the scope of the processed data

— information on the methods of data collection and disclosure – information on the recipients or categories of recipients to whom the data may be transferred

— a description of the technical and organisational security measures

— information relating to any possible data transfer to a non-EEA country.

18. Exemptions from registration

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.

According to the amended Data Protection Act, the data controller is exempt from the obligation to notify and register databases if he/she appoints the Data Privacy Officer. Also, the obligation to register a data filing system does not apply when such data are processed exclusively in the paper version of data files.

19. 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.

20. Data protection rights and remedies

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.

21. Sanctions for non-compliance

(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:

— remedy the negligence

— complete, update, correct, disclose or not disclose personal data

— apply additional measures to protect the processed data

— suspend data flow to a third country (and thus suspend a project)

— 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 to 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 takeovers, 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.

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

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

CMS Cameron McKenna
Greszta i Sawicki sp.k.
Warsaw Financial Centre
Ul. Emilii Plater 53
Warsaw - 00-113
Poland

T +48 22 520 5555
F +48 22 520 5556

Romania

1. Applicable law

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 by data controllers established in 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 foreign data controllers must appoint a representative in Romania.

2. The data protection authority (DPA)

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. Appointment of internal data protection officers

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. Internal privacy policies and external privacy notices

Under the Data Protection Act, data controllers 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 he/she 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. 'Personal data' and 'sensitive 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 special categories of data ('sensitive personal data') which include: (i) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, and (ii) personal data concerning health, addictions, sex life, or criminal record. The DPA also regulates specific categories of personal data the processing of which poses specific risks to the rights and freedoms of individuals – these categories include those specified above, as well as others (e.g. processing of data through electronic means for the purposes of evaluating certain aspects of the individual's personality such as professional competencies, credibility, behavior etc.; processing of personal data through electronic means for the purposes of taking an automated decision with respect to the solvency, financial-economic situation of the individual or to any acts which may entail the disciplinary, administrative or criminal liability of individuals). In these cases, a prior audit by the DPA of the data processing activities is mandatory, prior to commencement of the data processing activities.

6. The minimum age for collection of personal data

There is no minimum age for the collection of personal data, assuming applicable legal safeguards are implemented. The processing of personal data about minors, within direct marketing activities, or data about minors collected through the internet or electronic communication means, is expressly regulated as processing that poses specific risks to the rights and freedoms of individuals and is subject to a mandatory DPA audit prior to commencing processing activities.

7. Consent requirements (general, special categories and marketing)

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 is required to outline 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.

8. Processing without 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.

9. Data transfers

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. Under Data Protection Act such transfer requires the controller/processor to submit a prior notification to the DPA. DPA decision No. 200/2015 appears to ease such requirement. The same remains true for transfers to third-party data importers located in non EU/EEA countries but to which the DPA has recognised a similar level of protection (e.g. Switzerland, Jersey, Guernsey, Isle of Man, Canada and Argentina).

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

— the transfer is expressly approved by the relevant persons whose data will be transferred, or

— 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.

In 2014 the DPA adopted specific BCR local legislation. Such transfers under Binding Corporate Rules nevertheless require specific prior authorisation from the DPA. In the case of US recipients which have implemented the Safe Harbor principles, the DPA's position has been no prior authorisation is needed (however, in practice, the DPA did require the data controller to provide proof that the personal data recipient holds Safe Harbor certification). Following the recent ECJ judgment invalidating the European Commission's Decision no. 2000/520/EC acknowledging an adequate level of protection for US data recipients holding a Safe Harbor certification, the Romanian DPA has announced that it will no longer register transfers of personal data to US entities on the basis of Safe Harbor principles. Consequently, after the date of the ECJ decision, transfer to US data recipients may be done only on the basis of the other transfer guarantees provided by the law, such as standard model clauses or Binding Corporate Rules. Moreover, the Romanian DPA has indicated that data controllers whose processing operations have already been registered in the Registry of Personal Data Processing may continue to transfer personal data to the US only on the basis of such safeguards.

10. Intra-group transfers

A group company is regarded as a third party, and, as above, would either (i) need to independently satisfy the legal requirements for processing personal data, or (ii) 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.

11. Mandatory data protection information

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:

— the voluntary or mandatory nature of the data processing

— a list of the personal data processed

— the purpose and legal basis of data processing

— who the data controller(s) and the data processor(s) are

— the duration of the processing of the data

— who has access to the data

— if any data are transferred to a third country

— the rights and remedies of the relevant persons, and

— 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.

12. Notice & consent language requirements

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 the Romanian Constitution the official language is Romanian, the Romanian language is expected in relation to notice and consent.

13. Appointment of data processors

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.

14. Data retention

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/data retention 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, safekeeping 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.

15. 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 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.

16. Other specific obligations

In all cases, as per the Data Protection Act the DPA must at the very least be notified of any transfer of data outside Romania. For transfers to EU/EEA data recipients (or to other third party countries for which the DPA has recognised an adequate level of protection, now including also all US transfers, irrespective of Safe Harbor certification), the transfer must also be approved by the DPA, which will conduct a verification of the legitimacy of the data transferred and shall assess 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 in these cases, it is necessary to wait for the DPA's feedback/authorisation. Pursuant to the law, 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. In practice, this deadline is often exceeded, which is why transfers abroad to such third-parties must be thought out and planned well in advance of the envisaged implementation date, so as to ensure that all prior authorisations are in place.

17. 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. DPA decision No. 200/2015 appears to simplify such notification requirement. The registration procedure requires the completion of the standard online forms of the DPA (to be followed by a hard paper original of the signature page) and it is currently free of charge. Other than the categories of sensitive data in respect of which the data controller must mandatorily await the prior audit of the DPA (and the conclusions thereof), the Data Protection Act provides that processing may commence if the DPA has not notified the applicant within 5 days of the filing date as to the fact that it intends to initiate a prior audit.

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

18. Exemptions from the registration

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

— keeping a registry designed for public information

— claims submitted by petitioners to public authorities, that are to be reviewed as part of such authorities' legal obligations

— employees and external collaborators, to comply with a legal obligation or for the purposes of subscription of shares in the employees' interest

— owners or tenants, by owners or tenants associations

— the economic-financial, public relations or administrative activity of public or private companies

— individuals who participate in a contest or exam for hiring purposes, or who submit their resumes in this regard

— individuals participating in conferences or seminars, provided that the processing relates exclusively to data necessary for the organization of such events

— members of associations or NGOs for the purpose of performing their activities, without disclosure to third parties

— clergy activities

— 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

— journalistic, literary or artistic purposes

— individuals performing an independent activity (such as lawyers)

— use of the National Archives database, or use by libraries

— activities of courts of law

— real estate intermediation activities

— members of political parties, provided that such data is not disclosed to third parties without consent of the data subject

— personal data of contact persons, processed by data controllers exclusively for the purposes of their professional activities, by keeping a record of contact details thereof.

19. Specific notification obligations

The processing of certain categories of data requires notification to the DPA and a mandatory prior investigation by the DPA as to whether the processing does not violate the rights and freedom of individuals. Such categories of data include:

— 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.

20. Data protection rights and remedies

In line with Article 12 (*Right of Access*) of Directive 95/46/EC, the data subject 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 15 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:

— it is processed unlawfully

— the relevant person makes such a request

— it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by law

— the purpose of processing no longer exists or the legal time limit for retention has expired

— 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:

— 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

— if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research, and

— 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.

21. Sanctions for non-compliance

(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:

— order the rectification of any personal data that is deemed inaccurate

— order the blocking, erasure or destruction of personal data processed unlawfully

— prohibit the unlawful handling or processing of personal data

— prohibit the cross-border transmission or disclosure of personal data

— order access to the relevant person's information, if it was refused by the data controller unlawfully or

— impose a fine of between RON 500 (approx. EUR 111) and RON 50,000 (approx. EUR 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. In the electronic communication sector, companies with a turnover in excess of RON 5 million (approx. EUR 1.1 million) may be subject to a fine up to 2% of their turnover.

(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

Since 1 February 2014, certain unlawful data processing is punishable by imprisonment or by penal fine under the New Romanian Criminal Code.

Unlawful data processing relates to unauthorised use of images of a person, or unauthorised recording of the voice of a person. Imprisonment ranges from one month to five years, while the penal fine would may be up to RON 120,000 (approx. EUR 27,000).

Gabriel Sidere
Managing Partner
T +40 21 407 3813
E gabriel.sidere@cms-cmck.com

Marius Petroiu
Senior Associate
T +40 21 407 3889
E marius.petroiu@cms-cmck.com

Cristina Popescu
Senior Associate
T +40 21 407 3811
E cristina.popescu@cms-cmck.com

CMS Cameron McKenna SCA
S-PARK, 11-15 Tipografilor Str.
B3-B4, 4th Floor
District 1, 013714
Bucharest, Romania

T +40 21 40 73 800
F +40 21 40 73 900

Russia

1. Applicable law

Federal Law No. 152 – FZ 'On personal data' dated 27 July 2006, in effect since 27 July 2011, ('Data Protection Act') subject to numerous amendments, is based on the Strasbourg Convention of 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Strasbourg Convention') and provides a general framework for data protection. To be more precise, it defines personal data and data processing, regulates consent rules, cross-border data transfers, the obligations of data controllers and the rights of natural persons. There are also several legislative acts which contain some sector-specific privacy and security requirements (for example, the Labour Code contains some provisions on the 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 data processing measures.

2. The data protection authority (DPA)

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

3. Appointment of internal data protection officers

The DPA provides that all legal entities that deal with personal data should appoint a person responsible for the organisation's compliance with the laws regulating data processing. However, no specific requirements are provided by the Data Protection Act with regard to the specific qualifications required from such person.

The Data Protection Act stipulates that a person responsible for the organisation's compliance with data protection laws shall:

— exercise internal control over the data controller's and its employees' compliance with Russian legislation on personal data, including the requirements of personal data protection

— inform the operator's employees regarding the provisions of Russian legislation on personal data and local acts on issues regarding data processing and the requirements of personal data protection

— organise the acceptance and processing of applications and individual requests of data subjects or their representatives regarding their personal data and/or exercise control over the acceptance and processing of such applications and inquiries.

4. Internal privacy policies and external privacy notices

Under the Data Protection Act, data controllers are obliged to produce regulations on data processing and make them accessible to the public (e.g. publish them on a web-site). The regulations should determine the procedures for avoiding violations of legislative provisions relating to personal data protection and the measures aimed at eliminating the negative consequences of such violations of the law.

5. 'Personal data' and 'sensitive data'

Like the Strasbourg Convention, the Data Protection Act does not provide an exhaustive list of data which is deemed to be '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 defines 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 the state of health, sex life, and criminal record of a natural person.

6. The minimum age for collection of personal data

The Data Protection Act does not contain such a specification. In accordance with the general civil code parents or other legal representatives are allowed to act on behalf of children under 18 years of age and to give consents to the processing of their personal data.

7. Consent requirements (general, special categories and marketing)

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. The data controller should always be able to prove (in the case of any ambiguity) that the consent has been provided properly and lawfully. That is why obtaining consent in an electronic form or verbally remains somewhat risky for being able to prove that 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:

— processing of sensitive personal data

— 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 should 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 data controller

— purposes for processing the personal data

— list of the personal data to be processed to which the consent is given

— name and address of the technical processor which processes the personal data at the request of a data controller (if applicable)

— list of operations that will be performed with the personal data, the general description of the methods that will be used for the 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).

The Data Protection Act does not provide for any specific requirements for consent to the processing personal data for marketing purposes. Marketing agencies and sellers shall ensure that the consent of individuals to the receipt of such materials is obtained (opt-in).

8. Processing without consent

The Data Protection Act provides a list of ten 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 the execution of a court decision.

The same applies to cases where the processing of 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 data controller's legal interest and socially important causes, under the condition that the rights of the relevant person are not violated.

The relevant person's consent is also not required for the execution of the powers of federal executive authorities, state non-budget funds, the executive authorities of subjects of the Russian Federation and local authorities as well as the functions of the organisations taking part in the provision of state and municipal services, including the registration of a personal data subject in the integrated portal for state and municipal services and/or the regional portals for state and municipal services.

This exception also applies to situations where personal data is required for the execution and/or signing of a contract to which the relevant person is a party, beneficiary or guarantor, in particular if the operator exercises its right to assign the rights (claims) under the

given contract. 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 example is 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 causes (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 a disclosure of personal data in accordance with the requirements of the law may also be performed without the consent of the relevant person.

9. Data transfers

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 the 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 has been adopted by the 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 7 above.

10. Intra-group transfers

A group company is regarded as a third party. As above, the transfer of data to another member of the company group would either need to independently satisfy the legal requirements for the 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. It is recommended to include specific security and confidentiality provisions with respect to the personal data in transfer agreements between the group companies.

11. Mandatory data protection information

Before the commencement of the data processing the data controller, upon the request of the relevant person, should provide the relevant person with clear and detailed information regarding all of the circumstances in relation to data processing, including:

- confirmation that his/her personal data is processed by the data controller
- the legal grounds and purposes for processing the personal data
- the purposes and methods of processing personal data used by the data controller
- 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 with the law
- a list of the personal data processed referring to the corresponding subject of the personal data, the sources from which the personal data were obtained, unless another way of obtaining the data is not allowed by the law
- the duration of the processing and the storing of the personal data
- the procedure for enforcement by the relevant person of his/her rights, provided by the law
- information on performed or intended cross-border transfers of personal data
- the name and address of the technical processor of personal data, if the data processing is assigned or will be assigned to such a person
- other information the disclosure of which is required under the law.

12. Notice and consent language requirements

The Data Protection Act does not specify the language in which the consents should be obtained in connection with data processing. However, according to the Data Protection Act the given consent should be specific, informed and conscious, so that the relevant person fully understands the essence of giving their consent. For this reason, in practice, it may be necessary to have a Russian translation of the consent. This will also help to avoid the risk that the consent could be considered void. Thus bilingual consent is recommended.

13. Appointment of data processors

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 a relevant agreement, which should contain the elements required by the Data Protection Act (such as, terms and purposes of the data processing, confidentiality and data security obligations of the processor, obligations of the processor to comply with the methods of protect provided by Data Protection Act, etc.). A company that processes personal data (the 'technical processor') should perform its activities in accordance with the requirements of the law, which includes ensuring the confidentiality and protection of the personal data.

14. Data retention

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 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 of the Data Protection Act, the duration of the processing of 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 the processing of 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.

15. 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 the devices on which personal data are stored (the form of such a 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 the unauthorised processing of personal data. It is also necessary for the data controller to establish the rules of access to personal data.

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 supplemented and amended.

16. Other specific obligations

A data controller must perform an internal audit and assessment of the effectiveness of the measures which are taken to protect personal data. The 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 or 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.

Starting from 1 September 2015 amendments to the Data Protection Act will become effective according to which a data controller will be required to ensure that the recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is to be conducted in databases located within Russia. It is confirmed by the DPA that these so called 'localisation rules' will not affect cross-border transfer of data, and the copies of data may be sent abroad, used and stored in foreign databases until legitimate goals of processing are achieved, and provided that the Russian rules of cross-border data transfers are observed at all times during such processing.

Some exceptions to this rule exist in connection with certain purposes of data processing. These include achieving the objectives of international treaties or laws, the implementation of an operator's statutory powers and duties, the administration of justice, the acts of public law entities and organisations that provide state and municipal services, the professional activities of journalists and/or the lawful activities of mass media, or scientific, literary or other creative activities provided that this does not violate a data subject's rights and legitimate interests.

17. Registration obligations at the DPA

Data controllers must submit a notification to the DPA of their intention to process personal data. The notification procedure requires the completion of standard online and/or paper forms which are 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 after a data controller has been registered. The DPA completes the registration within 30 days. After that, the information on the 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 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. Starting from 1 September 2015 the notification shall also include information on the localisation of the database containing Russian citizens' personal data. If any changes are made to the registration data, an application for the registration of the changes must be submitted to the DPA. The registry of data controllers is available for inspection at the following address: http://rkn.gov.ru/personal-data/register/

18. Exemptions from the registration obligations

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

- personal data of employees processed by an employer for employment purposes
- personal data received by a data controller in connection with 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
- 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
- personal data made public by the relevant person
- personal data which includes only names, surnames and patronymic names of the relevant persons
- personal data which is necessary for the organisation for a one-time entry of the relevant person to the territory of the controller (or for the similar purposes)
- 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
- personal data processed without the use of automatic methods, in compliance with the law
- personal data processed in accordance with regulations on transport security.

19. Specific notification obligations

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

20. Data protection rights and remedies

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 the processing his/her personal data, including confirmation that his/her personal data is processed, the legal basis, purposes 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 the processing (including duration of storage), information on cross-border transfers of personal data, information on the technical processor of the personal data, on the procedure for the relevant person to realise 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 any personal data that is false.

Deletion

Personal data must be deleted (with the exception of data processed on the basis of a legal requirement to do so) in the following cases:

- upon the request of the relevant person
- if the personal data is deficient, outdated, inaccurate, or was illegally obtained and is not necessary for the declared purpose of the processing
- if the purpose of the processing is achieved, or the purpose is no longer relevant.

Blocking

If the 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 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 to a court in case of the unlawful processing of his/her personal data.

21. Sanctions for non-compliance

(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:

— to request the data controller to rectify the violation of the data processing, or

— to issue a warning to the data controller, or

— to impose the following fines for violations of data processing:

  - RUB 300 – 500 (EUR 7.5 – 12.5) on individuals
  - RUB 500 – 1,000 (EUR 12.5 – 25) on officials of legal entities
  - RUB 1,000 – 5,000 (EUR 25 – 125) on legal entities.

The Bill amending the laws which aim at substantially increasing the fines is currently under examination with the State Duma (Russian Parliament). The Bill proposes to replace the generally worded administrative offence of breach of personal data law with the following more clearly defined offences:

— Illegal processing of sensitive personal data - RUB 150,000 - 300,000 (approx. EUR 2,270 - 4,540).

— Data processing without the consent of the relevant person or persons ('data subjects') - RUB 30,000 - 50,000 (approx. EUR 455 - 760).

— Breach of the secure storage rules for tangible media objects (where personal data is processed otherwise than by automatic means) - RUB 25,000 - 50,000 (approx. EUR 380 - 760).

— Failure to comply with the requirements on written consent to data processing - RUB 15,000 - 50,000 (approx. EUR 230 - 760).

— Failure to amend, block access to or destroy personal data at the legitimate request of a data subject or competent authority - RUB 25,000 - 45,000 (approx. EUR 380 - 680).

— Failure to provide a data subject with information on the processing of his/her personal data - RUB 20,000 - 40,000 (approx. EUR 300 - 600).

— Failure to publish or otherwise make publicly available the data processing policy or information on its implementation - RUB 15,000 - 30,000 (approx. EUR 230 - 460).

Moreover, the DPA shall create a 'Register of the Violators of the Personal Data Subjects' Rights' by 1 September 2015. This Register, on the basis of a court judgment, will include information about data controllers violating personal data subjects' rights on the Internet. Inclusion of controller in the Register means that access to its domain names or other links to web-site pages on the Internet containing information processed in violation of the Data Protection Act will be restricted. Creation of such a Register is foreseen by the law which adapts the new 'data localisation rules'.

(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 to be an 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.

Leonid Zubarev
Senior Partner
T +7 495 786 30 85
E leonid.zubarev@cmslegal.ru

Vladislav Eltovskiy
Associate
T +7 495 786 41 36
E vladislav.eltovskiy@cmslegal.ru

CMS, Russia
Naberezhnaya Tower,
block C
Presnenskaya
Naberezhnaya 10
123317 Moscow

T +7 495 786 4000
F +7 495 786 4001

Slovakia

1. Applicable law

Act No. 122/2013 Coll. on the Protection of Personal Data as amended by Act No. 84/2014 Coll. ('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 security measures and regulation No. 165/2013 on the inspections of the data protection official were adopted to execute the Data Protection Act.

To be more precise, the Data Protection Act defines the protection of the personal data of natural persons during the course of the processing of their data, principles of data processing, security of personal data, protection of the rights of individuals, trans-border data transfers, registration and maintenance of records of filing systems and databases. The Data Protection Act can be found at the following link:

http://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/136_2014.pdf (only available in Slovakian).

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

The Data Protection Act also applies to data controllers, whose registered office or permanent residence is not in:

— the Slovak Republic but is located abroad where the laws of the Slovak Republic take precedence based on international public law

— a Member State of the European Union, provided that for the purposes of data processing they use fully or partially automated processes other than the automated means of processing located in the Slovak Republic, provided that such means of processing are not used solely for transferring personal data through Member States of the European Union.

2. The data protection authority (DPA)

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 ('DPA'). The DPA's website can be found at the following link http://www.dataprotection.gov.sk

3. Appointment of internal data protection officers

Data controllers are responsible for the internal supervision and protection of personal data processed within their organisation. 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 data protection officer.

A data controller may decide to appoint a data protection officer or multiple data protection officers in writing to monitor compliance with the Data Protection Act. If the data controller decides not to appoint a personal data protection officer he/she must notify the DPA of all of the filing systems in which personal data are processed. The duty of special registration of filing systems is not affected by the appointment of a data protection officer. The data protection officer must pass the exams prescribed by the DPA.

The basic duties of the 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 such violations, to implement the technical, organisational and personal measures needed, to carry out internal supervision monitoring the fulfilment of the controller's basic obligations and to internally supervise cross-border personal data transfers and to register or change or deregister the relevant filling systems with the DPA. A data controller who appointed a personal data protection officer has to register such a person with the DPA within 30 days from the day of the appointment.

4. Internal privacy policies and external privacy notices

It is common for companies, especially multinational companies who process cross-border data transfers both within and outside of their company group, to introduce internal privacy policies and publish publicly available privacy notices.

5. 'Personal data' and 'sensitive data'

Similarly to Directive 95/46/EC, the Data Protection Act does not provide for an exhaustive list of data which shall be deemed to be '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 or general identifier or by reference to one or more factors specific to the individual's 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. When processing personal data, an individual's birth number may be used only for identification purposes provided that its use is necessary for achieving the given purpose of the data processing.

Personal data relating to a breach of provisions invoking criminal or civil liability, may only be processed by a person entitled to process such data 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 the processing is necessary to achieve that purpose, and such processing expressly results from a special act, or written or equivalent 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 a third party.

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

Adequacy, necessity and legal basis of biometric data processing is determined by the DPA in the procedure contained in Sections 37 to 39 of the Data Protection Act.

6. The minimum age for collection of personal data

Act No. 40/1964 Coll. on the Civil Code regulates legal age as follows:

— The full capacity of an individual to acquire rights and assume duties on the basis of their own legal acts (capacity to perform legal acts) shall arise at the moment of his or her maturity. Maturity shall be acquired by achieving the age of eighteen. Before achieving this age, maturity can be acquired only by marriage. Maturity acquired in this way cannot be lost even if the marriage becomes extinct or if it is declared invalid by a court.

— Minors shall be capable only of such legal acts which are appropriate to the maturity of their reason and will with regard to their age.

Data controllers need to decide on a case-by-case basis whether granting consent to processing personal data is adequate to the maturity of the reason and will of the data subject with regard to the age of the data subject. To reach sufficient level of legal certainty it is recommended to always obtain the consent of the legal representatives of data subjects who are minors.

7. Consent requirements (general, special categories and marketing)

The definition of data processing is very broad. The processing of personal data means any operation or set of operations which are performed on personal data such as obtaining, collecting, recording, organising, adapting or altering, retrieving, consulting, aligning, combining, transferring, using, storing, destroying, transmitting, providing, making available or making public data.

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 freely given specific and informed indication of his/her wishes by which the data subject knowingly signifies his/her agreement to personal data related to him/her being processed. In practice, 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' (opt-in). Prior to expressing acceptance by electronic means, the relevant person should be given an opportunity to read the relevant privacy policy. The Data Protection Act distinguishes between written consent and other types of consent. Processing of special categories of data requires written consent. Where written consent is required it may be granted only with the signature of the data subject or by means of a qualified electronic signature.

Even in cases where written consent is not required, the data controller should always be able 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 the computers of users with their prior consent. Consent also means that the user accepts the cookies by a respective setting of the web browser.

The controller shall process personal data without the data subject´s consent only if the subject of the processing is constituted solely of the title, name, surname and address of the data subject without the possibility of adding his/her other personal data and they are 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, the controller may provide the above personal data, without the possibility of making them available and public only if such data are provided to another controller whose scope of activities is also direct marketing solely for the purposes of direct marketing. The data subject shall be entitled to object to such data transfers through a written application.

For the purposes of direct marketing, the call or use of automated calling and communications systems facsimile machines, electronic mail, including SMS to the subscriber or user can only take place following the data subject's consent to such data processing, and such consent should always be provable. The consent given may be recalled any time. The prior consent of the recipient shall not be required for the direct marketing of similar products and services to those that the person has obtained as a result of which the contact information for the electronic mail delivery in relation to the product or service sale has been obtained in accordance with the Act No. 351/2011 Coll. on electronic communications.

8. Processing without consent

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

— the data are processed pursuant to a special act (e.g. the act on health insurance, the act on banks, etc.), an international treaty binding on the Slovak Republic or a directly enforceable and legally binding act of the European Union stipulating a list of personal data, the purpose of their processing and the group of the data subjects

— the processing of the 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 the processing is necessary under the scope of its activities

— 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 the negotiation of a contract at the request of the data subject

— the processing of the personal data is necessary for the protection of the life, health or property of the data subject

— the subject of the processing consists solely of the title, first name, surname and address of the data subject without a possibility of adding his/her other personal data and the data are to be used solely for the controller's mail correspondence with the data subject and the keeping of records of such data

— the processed personal data have already been made public legally

— the processing of the personal data is necessary for the fulfilment of an important task carried out in the public interest

— the processing of the personal data is necessary for the protection of the statutory rights and legitimate interests of the controller or a third party, mostly the personal data processed in relation to protection of property, financial and other interests of the controller and personal data processed for securing the safety of the controller by cameras or similar systems; this shall not apply if the fundamental rights and freedoms of the data subject protected by the Data Protection Act are predominant in such data processing.

In the above cases, personal data may also be processed if the relevant person withdraws its consent to data processing (which data subjects are entitled to do at any time). 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 it is processing his/her personal data. Also the controller should inform the data subjects of this fact the next time the data subjects are contacted, however, no later than within three months from the day the processor was engaged, if the data subject is not informed by the processor within this time period. Otherwise the DPA may impose a fine on the processor of EUR 1,500 to EUR 50,000.

9. Data transfers

The transfer of data to a member state of the EU has the same effect as if data was transferred within the Slovak Republic. A controller with its registered office, place of business or permanent residence in the territory of the Slovak Republic shall be obliged to adopt adequate safeguards to secure that the rights and interests of data the subjects protected by law.

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

Where the final destination country does not ensure an adequate level of protection for personal data, the transfer may only be executed on the condition that the controller has adopted the EC Model Clauses, or Binding Corporate Rules, unless:

— the data subject consented to the transfer knowing that the final destination country does not ensure an adequate level of protection

— the transfer is necessary for the performance of a contract between the data subject and the controller or for the negotiation of changes to the contract with the data subject, or for the establishment of pre-contractual measures upon the data subject's request

— the transfer is necessary to enter into, or for the performance of a contract concluded by the controller with another entity in the interest of the data subject

— the transfer is necessary for the protection of the data subject's vital interests

— the transfer is necessary or required by law to safeguard an important public interest or for the establishment, implementation or defence of legal claims arising by the operation of law or international treaty by which the Slovak Republic is bound, or

— the transfer relates to personal data, which are part of lists, or registers according to 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.

In the light of the Court of Justice of the European Union judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner, the United States of America shall also be considered third country not ensuring an adequate level of protection for personal data.

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

If the personal data are to be transferred to a country outside the EU that does not ensure an adequate level of protection for personal data 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 Binding Corporate Rules, then the transfer does not need to be approved by the DPA. 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 the data, the identification of data subjects, categories of the transferred data, and the time for which the data will be stored by the importer. The transfer agreement must be attached to the application. The DPA has 30 days to decide the application.

10. Intra-group transfers

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 if Binding Corporate Rules were adopted and the transfer agreement meets the requirements of the Data Protection Act, then the consent of the DPA to the transfer is not required.

11. Mandatory data protection information

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/her in advance of the following without being requested:

— identification data of the controller

— identification data of the processor

— the purpose of the data processing

— the list of the processed personal data

— identification of the person entitled to obtain the personal data

— advice on voluntariness or obligation to provide the requested personal data

— third parties, provided that it is expected or clear that personal data will be provided to (and further processed by) them

— group of recipients, provided that it is expected or clear that personal data will be made available to (but not processed by) them

— form of making the data public, provided that personal data are to be made public

— third countries, provided that it is expected or clear that personal data will be transmitted to these countries

— advice on the existence of the data subject's rights.

Usually this information is provided to the data subject while obtaining consent for the processing of personal data directly in the text of the consent form. This information may also be provided to data subjects through the web page of the data controller.

12. Notice and consent language requirements

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, 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.

13. Appointment of data processors

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 contracts are specified in the Data Protection Act. If the controller engaged the processor with the processing after acquiring personal data it should inform the data subjects of this fact during the next contact, however, not later than three months from the day of the engagement of the processor, if the processor does not inform the data subject itself. This shall also apply if the data processing is taken over by another controller, e.g. in case of the merger of two controllers.

The processor shall inform data subjects that it was authorised by the controller to process the personal data of the 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 their consent to such provisions of data.

14. Data retention

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 retaining such data can be proved, 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.

Regarding 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.

15. Mandatory technical, organisational or security measures

Regarding 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, unauthorised access and publication, as well as against any other unauthorised 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 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 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. Security Project is mandatory for filing systems connected to publicly accessible networks if special category data is being processed, or if the filing system serves the fulfilment of public interest as defined in Section 3 subsection 1 of the Data Protection Act.

16. Other specific obligations

The controller is obliged to:

- determine the purpose of the processing of personal data before starting the processing of personal data
- determine the means and manner of the processing of personal data
- obtain personal data solely for a defined or determined purpose
- 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 achieving its purpose
- 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
- 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
- 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
- destroy the personal data whose purpose of processing has expired
- process personal data in accordance with good behaviour principles (i.e. no definition of good behaviour principles in Data Protection Act - according to the Slovak case law it is an action contrary to the ingrained traditions, e.g. honesty, good faith etc.)
- keep a record of the filing systems on his/her own, if a filing system does not need to be notified or registered with the DPA.

17. Registration obligations at the DPA

The Data Protection Act distinguishes between an obligation to maintain records of the filing system, an obligation to notify the DPA of the filing system and an obligation to undergo special registration of the filing system.

The notification obligation applies to all filing systems in which personal data are being processed by fully or partially automated means, unless:

- the filing system is subject to special registration; or
- the filing system is under the surveillance of the duly appointed data protection officer; unless the filing system in which personal data are processed according to Section 10, subsection 3, letter g.) of the Data Protection Act, which always have to be notified, or
- the filing system contains 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 or
- the filing system contains 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 is mandatory for filing systems in the following cases:

- personal data processed in relation to the protection of property, financial and other interests of the controller and personal data processed for securing the safety of the controller by cameras or similar systems; DPA decides whether notification or special registration is required on a case-by-case basis
- biometrical data is processed, unless there is an obligation of the controller to process such data stipulated by the Data Protection Act
- at least one of the special category data is processed, and at the same time their transfer to a third country not ensuring an adequate level of protection is expected.

The controller shall notify or register the filing system, if applicable before the commencement of the processing of personal data in the filing system. The notification may be given by electronic means using the standard DPA form. Assignment of an identification number to the filing system and issuance of a confirmation of its notification by the DPA shall

constitute a part of the notification process. The controller may start to process the personal data in such filing systems upon the delivery of the notification to DPA.

In case of special registration, e.g. in case of transferring sensitive data to a third country not ensuring adequate level of protection, the filing system in which such data are stored must be registered prior to the transfer. The controller shall be entitled to commence data processing in the filing system submitted for the special registration only after the certificate of the special registration has been delivered to it by the DPA.

18. Exemptions from the registration

The Data Protection Act specifies what kind of filing systems have to be notified or registered.

As explained above the obligation to notify or 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 which are:

— subject to internal supervision of a personal data protection officer, who was appointed by the controller in writing (except the filing system in which personal data are processed according to Section 10, subsection 3, letter g.) of the Data Protection Act, which always has to be notified). The DPA may decide that a filing system in which personal data are processed according to Section 10, subsection 3, letter g.) of the Data Protection Act is subject to special registration

— 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

— 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.

The controller shall be obliged to keep records of the filing systems, which are not subject to registration or special registration, at the latest from the day of commencement of the processing of personal data in these filing systems. The records shall contain data in the extent pursuant to Section 35 Paragraph 1 of the Data Protection Act. A template of the records shall be published by the DPA on its website.

19. Specific notification obligations

The controller has specific notification obligations towards the DPA in the following cases:

— appointment of the data protection officer and changes to the appointment

— restrictions of the data subject's rights

— alterations of the data submitted for notification or special registration.

There is no general obligation in Slovakia to notify affected individuals or a regulator such as the DPA in case of a data breach. A data protection officer has to notify the controller in writing, without undue delay, of any breach of statutory provisions of the Data Protection Act. Current legislation focuses more on the prevention of a breach. However, the proposal of the EC Regulation on Protection of Personal Data introduces general notification obligation in its Articles, based on the concept of notification of personal data breaches pursuant to Article 4, subsection 3 of the Directive on privacy and electronic communications 2002/58/EC. Thus it is expected that the general notification obligation in Slovakia will be subject to changes in the upcoming months.

In the case of a data breach in the electronic communication sector, an enterprise which provides public services shall notify the Regulatory Authority for Electronic Communications and Postal Services (not the DPA) and the subscribers about the breach if the conditions under Act no. 351/2011 Coll. on electronic communications were fulfilled.

In the sector of the critical infrastructure providers a concept of cyber security was recently submitted by Slovak Government office for intergovernmental comments. According to the concept, it is expected that an act on cyber security shall be enacted, which would include the notification obligations of critical infrastructure providers.

20. Data protection rights and remedies

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

— information about the state of the processing of his/her personal data in the filing system, and if personal data about the data subject are processed or not

— exact information, in a generally intelligible form, about the source from which the controller obtained his/her personal data for their processing

— a copy of his/her personal data, in a generally intelligible form, which constitute the subject of the processing

— rectification of inaccurate, incomplete or not updated information, which constitute the subject of the processing

— destruction of his/her personal data and returning of the documentation containing the personal data, provided that the purpose of their processing was fulfilled

— destruction of his/her 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/her in writing at the latest within 30 days from the day of its receipt.

Objection

The data subject shall be entitled to object to the controller (free-of-charge in a written application):

— processing and using his/her personal data for the purposes of direct marketing;

— 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 legitimate reasons of an infringement of his/her rights and legitimate interests or shall submit the evidence of an infringement of his/her 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 such data as soon as possible

— to object and refuse the decision of the controller which may have significant implications for the data subject, if such decision was made only based on 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 if:

— the reasons, which prevented obtaining the 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)

— the controller is processing incorrect or inaccurate personal data

— 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/she 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 the 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/her 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.

21. Sanctions for non-compliance

(A) Administrative remedies and other sanctions

In case of a violation of the Data Protection Act by the controller or processor, the DPA may:

— impose an obligation to take, in a determined time limit, the technical, organisational and personal measures adequate to the manner of the processing

— prohibit the processing of the personal data, the processing of which is contrary to the provisions of the Data Protection Act

— order the removal or destruction of the personal data, in a determined time limit, provided that they are or were processed illegitimately

— impose on the controller an obligation to change the processor

— impose an obligation to develop or to update the Security Project or documentation

— 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

— impose a fine of EUR 300 up to EUR 200,000 (according to the type of breach, its severity and consequences).

Fines are categorised according to specific obligations breached:

— EUR 300 to EUR 3,000 (e.g. notification obligations, inaccuracy of data)

— EUR 1,000 to EUR 50,000 (e.g. basic principles, processor appointment, liquidation of data)

— EUR 1,000 to EUR 200,000 (e.g. data transfer to third countries, protection of special category data, special registration).

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 five 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 or the processor. The individual shall be entitled in particular to demand that the unlawful violation of his or her right to privacy be abandoned, that the consequences of this violation be removed and that an adequate remedy be given to him or her. If the remedy appears insufficient due to the fact that the individual's dignity or honour have been considerably reduced, the individual shall also have a right to a pecuniary satisfaction of the immaterial detriment. The amount of the pecuniary satisfaction shall be specified by the court with regard to intensity and the circumstances of the infringement.

(C) Criminal law issues

In serious cases, unlawful data processing may also be deemed to be, 'Unauthorised Use of Personal Data', 'Violation of the Privacy of Correspondence' or 'Dangerous Stalking' under Act No. 300/2005 Coll. Criminal Code which may be punished by imprisonment.

Adriana Kováčiková
Partner
T +421 2 32 333 431
E adriana.kovacikova@rc-cms.sk

Peter Bartoš
Associate
T +421 2 32 333 423
E peter.bartos@rc-cms.sk

Ružička Csekes s.r.o.
in association with members of CMS
Vysoka 2/B
811 06 Bratislava
Slovak Republic

T +421 2 32 333 431
F +421 2 32 333 443

Turkey

1. Applicable law overview

There is currently no specific data protection legislation in Turkey. However, various pieces of Turkish legislation (expanded upon in Section 6 below) contain general provisions which regulate the processing and protection of personal data, including:

— The Constitution of the Republic of Turkey dated 7 November 1982 (the 'Constitution')

— The Civil Code, Law No. 4721 (the 'Civil Code')

— Penal Code, Law No. 5237 (the 'Penal Code')

— Code of Obligations, Law No. 6098 (the 'Code of Obligations') and

— Various sector specific legislation.

The provisions of the above laws constitute Turkey's regulatory framework for data protection and lay down the general rule that the illegal processing of personal data is prohibited and perpetrators may be subject to civil and criminal sanctions. However, what constitutes 'illegal processing' is unclear. Moreover, compliance with these provisions cannot be assured as no authority is responsible for monitoring compliance (see Section 2 below).

This legal environment is expected to change significantly in the future when the Turkish parliament ratifies the Draft Law concerning the Protection of Personal Data (the 'Draft Law'), which is expected to introduce registration and processing requirements similar to those of EU Directive 95/46/EC as part of Turkey's accession process for becoming a member of the European Union. Turkey, as a member of the Council of Europe, has already signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) in 1981, but has not ratified it yet.

2. Regulatory body and registration

There is currently no government body or organisation responsible for regulating the processing and protection of personal data in Turkey and consequently there is no requirement under Turkish law for entities handling personal data to register with, file or notify a data protection authority.

However, should the Draft Law come into effect, it is likely that registration obligations will be imposed and that an independent authority called the Personal Data Authority will be established to regulate and ensure compliance with the Draft Law.

3. Data protection officer

There is currently no requirement to appoint a data protection officer and the Draft Law is not expected to introduce such a requirement.

4. What is personal data?

Due to the absence of specific legislation, there is no universal definition of 'personal data', however some regulations have defined personal data within their specific context. For example, the Regulation on Protection of Personal Data in Electronic Communications Sector defines personal data as any '*information regarding a known or identifiable natural or legal person*'. Similarly, there is no specific definition of 'sensitive data', but the Penal Code imposes penalties on persons who record or process information relating to the medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sex life of an individual.

The Draft Law defines personal data as any information relating to an identified or identifiable natural and legal person and defines sensitive personal data as personal data revealing race, political opinions, philosophical beliefs, religion, sect or other beliefs, foundation or union membership, and the processing of data concerning health or private life and all kinds of convictions.

5. Transfer of data abroad

Other than the general provisions described in Section 6 below, there are no specific provisions concerning the transfer of personal data abroad. However, the general requirement to obtain the data subjects' prior consent will continue to apply and as a result organisations cannot transfer personal data abroad without obtaining prior consent from the data subjects.

Under the Draft Law, organisations will need to obtain approval from the newly established Personal Data Authority in order to be able to transfer personal data abroad, and approval which will only be granted where either:

— the recipient country provides an adequate level of protection, or

— where adequate protection cannot be established, where the data subject has granted consent to the transfer, or

— the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject.

6. Current general legal provisions

The Constitution

The protection of personal data has been enshrined as an individual right under the Constitution since 2010. Article 20 of the Constitution regarding the confidentiality of private life provides that everyone is entitled to the protection of their personal data and gives individuals the right to be informed of, have access to and request the amendment and deletion of his or her personal data. Personal data can only be processed after obtaining the express consent of the individual or otherwise in accordance with the law. There is no further explanation as to how such consent shall be obtained, but it is generally accepted that the consent shall be in writing and voluntary and shall identify the purposes of processing personal data.

It is further stipulated that the principles and procedures regarding the use of personal data are to be further regulated by legislation. However, as mentioned above, such a law has yet to be enacted.

Civil Code

The Civil Code emphasises the consent requirement established by the Constitution by labeling any violation of personal rights unlawful unless there is consent, superior private or public benefit or authority granted by law. There is monetary remedy available for individuals whose personal rights are violated.

Penal Code

Articles 134-140 of the Penal Code regulate the protection of privacy and make it an offense to violate the confidentiality of private life. Article 135 specifically regulates the recording of personal data and states that persons who record personal data in a manner contrary to law shall be sentenced to imprisonment for between one-to-three years and those distributing, or obtaining personal data to or from another person contrary to law can be sentenced to imprisonment for between two-to-four years.

The Penal Code specifically restricts the recording and processing of sensitive personal data relating to the medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sex life of an individual.

The investigation and the following prosecution under the Penal Code may only be initiated if a complaint is filed by the injured party within six months as from the date of the alleged crime occurred. If the violating party is a legal entity, it may be subject to an administrative fine and if it operates in a sector which requires a license (such as banking etc.) its license or permit may be revoked.

Code of Obligations

The Code of Obligations stipulates that an agreement which is contrary to personal rights shall be invalid, and that any person whose personal rights have been violated shall be entitled to claim damages. It also restricts the personal data which employers can use to an employee's qualification information and any other information which is required to perform a service.

Sector specific legislation

In addition to the general provisions described above, there are also sector-based laws, in particular applicable to the banking, healthcare, insurance and telecommunication sectors. Entities operating in these sectors should take these sector-based laws into consideration when operating in Turkey.

In particular, all employers should be familiar with the data protection provisions in the Labour Law, Law No.4857 (the 'Labour Law'), which provides that employers cannot disclose information relating to their employees where it is in the employee's interest for the information to remain confidential.

John Fitzpatrick
Senior Partner, Turkey
T +90 212 243 4928
E john.fitzpatrick@cms-cmck.com

Alican Babalıoğlu
Partner
T +90 212 243 49 28
E alican.babalioglu@ybb-av.com

CMS Danişmanlik
Hizmetleri Avukatlik Ortakliği
Süzer Plaza,
Askerocağı Caddesi No:6
Kat:15 D:1501
34367 Elmadağ/Şişli–
Istanbul, Turkey

T +90 212 243 49 28
F +90 212 243 49 38

Ukraine

1. Applicable law

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 data processing in Ukraine. The Data Protection Act can be found in Ukrainian at the following link: http://zakon4.rada.gov.ua/laws/show/2297-17.

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 data processing that take place in Ukraine, including the cross-border transfer of personal data, are within the ambit of the Data Protection Act.

2. The data protection authority (DPA)

Under the Data Protection Act, powers of the special state agency in domain of personal data protection matters are delegated to the Ukrainian Parliament Commissioner for Human Rights (in Ukrainian – Уповноважений Верховної Ради України з прав людини, further - the 'Ombudsman'). The Ombudsman's web-site can be found at http://www.ombudsman.gov.ua/ua/page/zpd/obrobka/.

3. Appointment of internal data protection officers

By law, all state and municipal authorities, as well as all data controllers and processors who process personal data that constitute a special risk to the rights and freedoms of the data subjects ('High Risk Data') (see more details below) 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.

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 tasks and functions and has the following rights:

— informs and consults data processors or controllers on various matters relating to compliance with personal data protection laws

— interacts with the Ombudsman to prevent and eliminate violations of personal data protection laws

— secures enforcement of legitimate rights of the data subjects

— has access to any data being processed by the data controller or processor and to all premises of the data controller or processor where data processing takes place

— if any violations of data processing laws are revealed, informs data controllers or processors accordingly in order to take appropriate measures and

— analyses any threats for personal data security.

Data controllers or processors who process High Risk Data must notify the Ombudsman of the officer or structural subdivision who is responsible for personal data protection matters.

In companies other than those who process the High Risk Data, officers responsible for personal data protection shall be the same officers who are directly involved in the processing of personal data. If necessary, such companies are free to appoint separate officers or even create structural divisions that will be responsible for personal data protection matters. No notification requirements apply if the processing of the High Risk Data is not involved.

All persons who, in connection with their job duties, have access to other persons' personal data, must sign a non-disclosure undertaking.

4. 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. 'Personal data' and 'sensitive 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, criminal sentences, data concerning the health or sex life of the relevant persons and genetic data.

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:

— accusations of committing crimes

— rulings of the courts

— 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.

The Data Protection Act also introduces the notion of the High Risk Data, the processing of which may be carried out subject to notification of the Ombudsman.

In its scope, the High Risk Data to some extent (but not fully) overlaps with sensitive data. In particular, the High Risk Data includes data on racial, ethnic or national origin; political views; religious beliefs; worldview convictions (e.g. feminism, pacifism, vegetarianism); membership in political parties, trade unions, religious organisations or worldview-based non-governmental organisations; health condition; sex life; biometric data; genetic data; information whether a person has been brought to administrative or criminal liability; information whether a person was subject to pre-trial inquiry measures; information whether a person was subject to measures provided in the Law of Ukraine On Operational and Investigative Activities; information whether a person was subject to certain types of violence; location and/or routes of travelling of a person.

6. The minimum age for collection of personal data

In the Ukraine, there is no minimum age for the collection of personal data.

7. Consent requirements (general, special categories and marketing)

Generally, a data controller must always obtain explicit voluntary 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, through electronic communication 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.

The data controller must keep the documents or information confirming consent of the relevant person for the processing of his/her personal data during the entire period of such processing.

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 data processing is common for all types of data.

As regards advertising, including direct marketing, general rules regarding consent apply to relations of the advertiser/advertising company and recipient of advertising. There are no specific opt-in/opt-out requirements in connection with advertising/direct marketing in the Ukraine. But under the general provisions of the Data Protection Act an advertising addressee, as any person whose data is being processed, must be asked for consent for his/her data processing and should be able to recall his/her consent at any time. Therefore, we recommend companies engaged in direct marketing in the Ukraine to implement an opt-in/opt-out regime even if it is not no expressly required under applicable local laws.

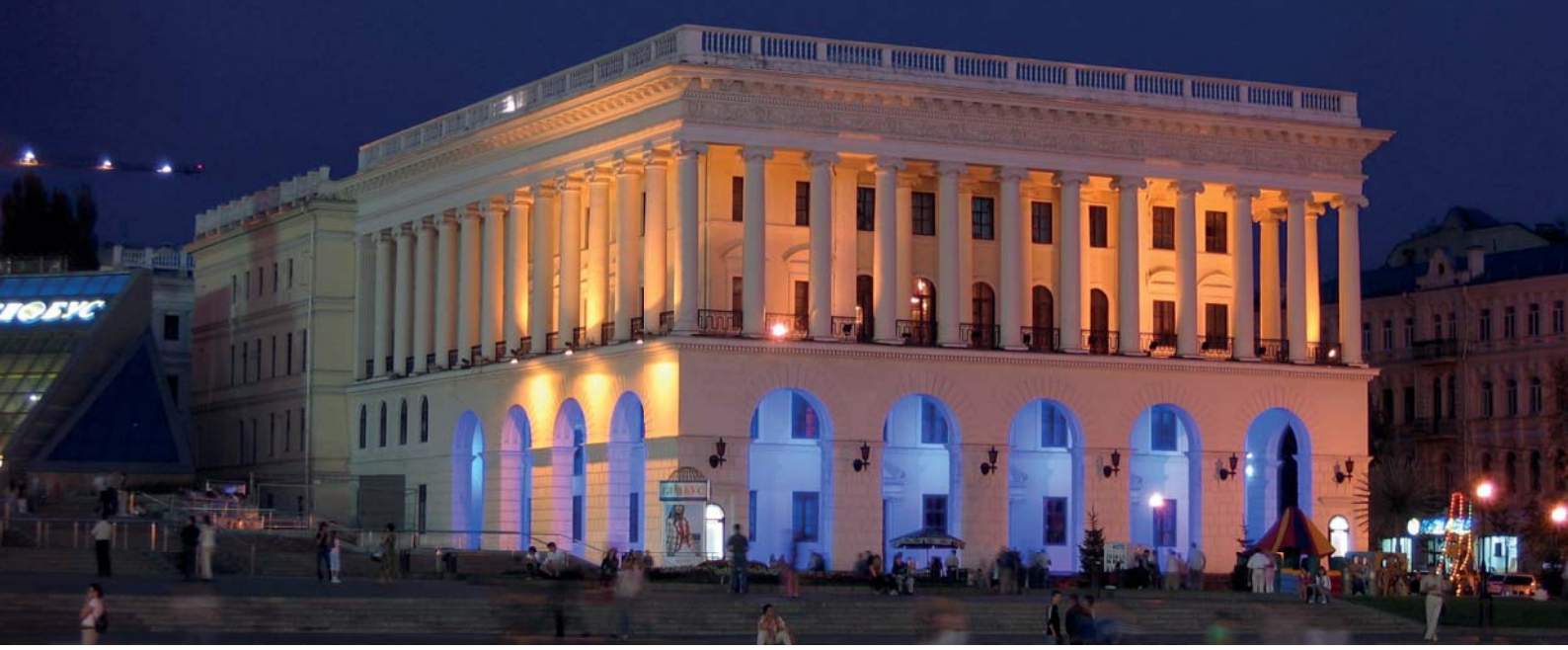
8. Processing without consent

Processing personal data without the relevant person's consent is permitted only in exceptional cases specifically provided for by law, which are as follows:

— where a permit for the processing of personal data is granted to the data controller by law exclusively for the performance of its authorities

— where personal data is being processed in connection with (i) conclusion or performance of an agreement to which the relevant person is a party or which is concluded for the benefit of the relevant person or (ii) taking measures that precede the conclusion of an agreement per request of the relevant person

— where data processing is necessary to protect vital interests of the relevant person



— where data processing is necessary for the due performance of the data controller's obligations as provided by law or

— where data processing is necessary to protect legitimate interests of the data controller or third parties to which the personal data is transferred, except for the cases when necessity to protect basic rights and freedoms of the relevant person (data subject) overcomes such interests.

Further, the law permits 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.

9. Data transfers

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 only possible if one of the following conditions is met:

— the relevant person has granted his/her express consent to such transfer

— the data controller and a relevant person need to enter into or perform an agreement for the benefit of the relevant person

— the data transfer is necessary to protect the vital interests of the relevant person

— the data transfer is necessary to protect the public interest or pursue legal remedies

— 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.

10. Intra-group transfers

Ukrainian law provides the same requirements with respect to the processing of 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).

11. Mandatory data protection information

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:

— the identity of the data controller

— the contents of the personal data being collected

— his/her rights granted by the Data Protection Act

— the purpose of the data collection

— 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 to the relevant person by the data controller or processor within thirty business days of collecting the personal data. There are no specific requirements regarding ways of communicating this information to the data subject. So both personal notification and privacy notice can equally work provided the data controller is able to prove that all necessary information has been made available to the data subject.

12. Notice & consent language requirements

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 the 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 language.

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 Ombudsman that the relevant person fully understood the conditions of consent and that the consent fully covers the scope and purpose of the data processing.

13. Appointment of data processors

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.

14. Data retention

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 it is required in order to achieve the legitimate purpose of the data processing.

Personal data must be destroyed in the following cases:

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

— termination of the legal relationship between the relevant person and the data controller/processor unless otherwise provided by law

— where there is a relevant warrant of the Ombudsman or authorised officers of the Ombudsman's office

— where there is a valid court judgment regarding withdrawal of the personal data from the database.

15. 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 accidental loss, destruction or unauthorised processing and access.

The data controller is responsible for undertaking all necessary security measures, including technical and organisational ones, to protect the data being processed in the database. For this purpose the data controller and processor, in their own discretion, determine a list and scope of measures aimed to secure the safety of the data processing. Such measures must be compatible with the requirements of data protection and information safety laws and regulations.

Organisational measures include:

— determining criteria for the access to personal data by the employees of the data controller or processor

— establishing a special procedure for recording operations relating to data processing and access to the personal data

— development of the action plan in case of an unauthorised access to personal data, technical equipment damages or emergency situations and

— regular trainings of the employees who work with personal data.

The data controller and processor must keep records of the employees who have access to the personal data of other persons. Further, the data controller or processor shall determine a level of access to the personal data in a way that each employee dealing with personal data could access only those data that are necessary for performance of his/her job duties. Each employee provided with access to other persons' personal data must sign a non-disclosure undertaking.

Once an employee dealing with personal data is dismissed or transferred to another position unrelated to data processing, his/her access to the personal data of other persons must be cancelled.

Further, the data controller and processor must keep records of the most important operations with respect to the personal data, including, the place and source of the personal data collection, changes to the personal data, any transfer or copying of the personal data, review of the personal data, date and time for retention or deletion of the personal data, identity of an employee who did any of the aforementioned operations, purpose of change, review, transfer, retention or deletion of the personal data. Information on the foregoing operations must be kept within a year following the calendar year when the relevant operation was completed unless other time periods are provided by applicable laws.

In addition to organisational measures, the data controller and processor must take special technical measures aimed at preventing an unauthorised access to the personal data.

16. 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 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:

— transfers of personal data upon requests arising from investigation and search operations or counterintelligence tasks, counter-terrorism activities

— performance by public authorities and local government bodies of their duties as provided by law

— data processing for historical, statistical or scientific purposes

— if the relevant person has already been provided with information on his/her data processing at the stage of data collection (see Section 11 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 etc.). The notification must be made within ten business days of the change or deletion.

17. Registration obligations at the DPA

There are no registration requirements under the Data Protection Act.

Please see details on mandatory notification to the Ombudsman on processing of the High Risk Data in Section 19 below.

18. Exemptions from the registration

N/A

19. Specific notification obligations

Data controllers processing the High Risk Data must notify the Ombudsman of the same. The notification must be submitted within thirty working days of when the data controller starts processing the High Risk Data.

No notification is required in the following cases of the High Risk Data processing:

— where processing is carried out by NGOs, political parties and/or organisations, trade unions, unions of employers, religious organisations, worldview-based non-governmental organisations, provided the processed data relates exclusively to the members of these unions/organisations and is not transferred without their consent

— where processing is carried out with the sole purpose of maintaining an open registry for the provision of information to the public

— where processing is necessary for the enforcement of rights and performance obligations of the data controller in the field of labour relations.

The notification is submitted according to the standard template approved by the Ombudsman.

Information on the processing of the High Risk Data is further published by the Ombudsman in the open public registry (at the date of this Guide this registry is not yet operating).

The data controller processing the High Risk Data must notify the Ombudsman of any change of the data that is subject to notification within ten business days after the relevant change occurred.

20. Data protection rights and remedies

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

— access his/her own personal data contained in the database

— 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

— submit an objection to the processing of his/her personal data

— set out certain restrictions/reservations with respect to any element of his/her data processing

— 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

— revoke his/her consent to the data processing.

21. Sanctions for non-compliance

Criminal and administrative liability for failing to comply with the data protection legislation is set out by 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 is not in compliance with the established order of personal data protection that resulted in unauthorised access to such personal data or other violations of the data subjects rights, the data controller could face a fine in an amount up to UAH 17,000 (ca. EUR 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.

Olexander Martinenko
Partner
T +380 44 391 3 704
E olexander.martinenko@cms-cmck.com

Nataliya Nakonechna
Senior Associate
T +380 44 391 3 729
E nataliya.nakonechna@cms-cmck.com

Olga Belyakova
Counsel
T +380 44 391 3 727
E olga.belyakova@cms-cmck.com

CMS Cameron McKenna LLC
6th Floor,
38 Volodymyrska Str.
01030 Kyiv, Ukraine

T +380 44 391 33 77
F +380 44 391 33 88

About us

Ahead of the curve

CMS represents your interests and advises you on all aspects of data protection and security, confidentiality, privacy, human rights and freedom of information law across industry sectors. You can rest assured that your matter is safe with us should it be about the use of data in relationships with employees, customers, service providers, agents, regulators and the general public, involving in connection with employee benefit arrangements, ICT infrastructures, contract centres, data warehousing arrangements, sales and claims operations and complaints processes and procedures. Our CEE Data Protection Team is providing a 'one-stop-shop' solution for you in data protection matters throughout the CEE.

CMS and the TMC sector

Our team offers you:

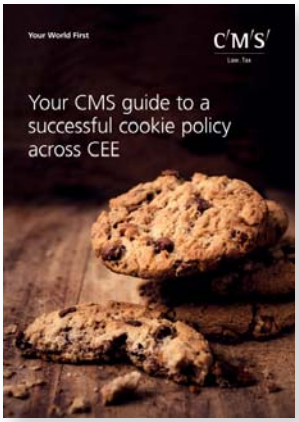
— Up-to-date advice on key privacy issues

— Dedicated privacy specialist across CEE in 17 countries

— A CEE footprint unrivalled by any of our peers

— Our lawyers are recognised as 'Leading Individuals' and practices are top ranked by independent legal directories

Further publication in data privacy




Mexico City
Rio de Janeiro
Aberdeen
Glasgow
Edinburgh
Hamburg
Amsterdam
Berlin
London
Utrecht
Duesseldorf
Leipzig
Bristol
Antwerp
Cologne
Brussels
Frankfurt
Luxembourg
Paris
Stuttgart
Strasbourg
Munich
Zurich
Geneva
Ljubljana
Lyon
Milan
Rome
Barcelona
Madrid
Lisbon
Seville
Algiers
Casablanca


Moscow
Warsaw
Kyiv
gue
nna
Bratislava
Budapest
Zagreb
Belgrade
Bucharest
Sarajevo
Sofia
Podgorica
Tirana
Istanbul
Beijing
Shanghai
Tehran
Dubai
Muscat

1511-0168-3