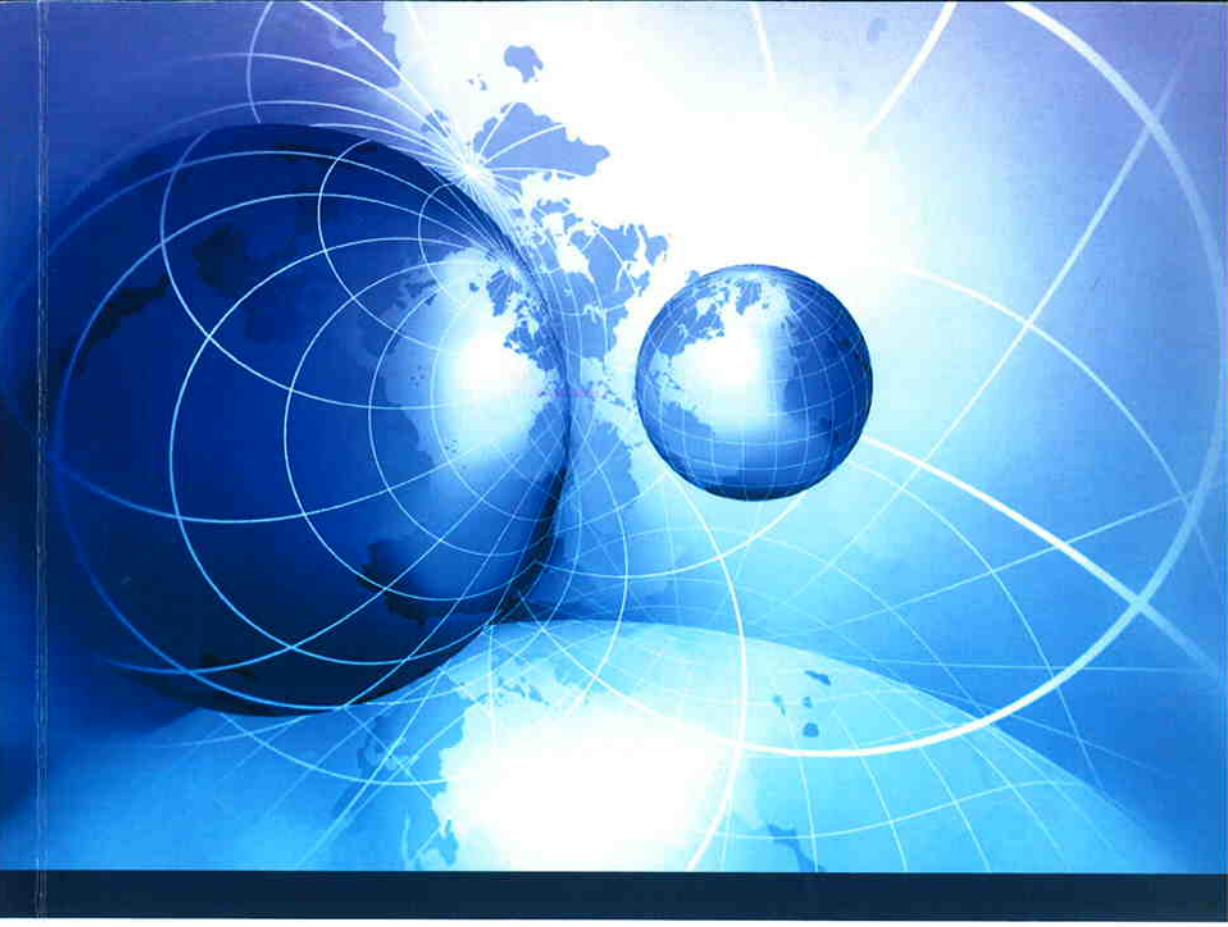

INTERNATIONAL PRIVACY GUIDE

NOVEMBER 2009

JARNO J. VANTO, ED.

WEST®

International Privacy Guide

By

Jarno J. Vanto, Editor in Chief

Volume 1, Number 1 **November 2009**

WEST®

A Thomson Reuters business

For Customer Assistance Call 1-800-328-4880

Mat #40886488

Czech Republic

*Petra Mirovská and Drahomír Tomašuk**

1. Introduction

1.1. Legal Framework

Protection of privacy is guaranteed by the Constitution of the Czech Republic and by the Charter of Fundamental Rights and Freedoms. Protection of personal data of natural persons in the Czech Republic is secured by the Personal Data Protection Act (the "Act"),[1] which came into force on 1 June 2000 and transposed Directive 95/46/EC of the European Parliament and of the Council (the "Directive")[2] into the Act.

---

*Petra Mirovská is an attorney at Kocián Šolc Balaštík (http://www.ksb.cz/). In her practice, she focuses on data protection, consumer protection law, litigation and arbitration, competition law and electronic commerce. She graduated from The Faculty of Law at Charles University in Prague where she received a doctorate in law in 2002. She also studied acquis communautaire at J.W. Goethe University in Frankfurt am Main, Germany. Petra has been a Czech advocate since 2006 and is a member of the Czech Bar Association.

She provides legal services in Czech, English and German. E-mail: mailto:pmirovska@ksb.cz.

Drahomír Tomašuk is an attorney at Kocián Šolc Balaštík. His practice involves telecommunications, data protection, banking, company law, and administrative law and proceedings. He holds a law degree from West Bohemian University in Pilsen (graduated in 1999). Drahomír has been a Czech advocate since 2003 and is a member of the Czech Bar Association. He provides legal services in Czech and English. E-mail: mailto:dtomasuk@ksb.cz.

Founded in 1990, Kocián Šolc Balaštík (KSB) is a leading independent law firm, one of the largest in the Czech Republic. Based in Prague with branches in Karlovy Vary and Ostrava, the firm provides fully integrated legal and tax advice to domestic and foreign clients through a team of almost seventy lawyers and tax advisers. KSB has repeatedly been named law firm of the year in the Czech Republic by independent rating agencies (Who's Who Legal Law Firm of the Year 2006–2009; Chambers Europe National Law Firm of the Year 2008).

[1]Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts, as amended.

[2]Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to processing of personal data and on free movement of such data.

The rights secured by the Act are complemented by the general privacy protection rules of the Civil Code, which state that natural persons have a right to protect their personality and privacy and documents of a personal nature, portraits, pictures, video and audio recordings of natural persons or personal expressions may only be taken or used with their consent, or for official purposes based on a special act and for scientific, artistic and press service purposes, as long as their legitimate interests are protected.[3]

In addition, certain provisions on protection of personal data can be found in other laws and regulations dealing with either specific situations, such as use of electronic communications,[4] provisioning of information society services[5] or processing of birth numbers,[6] or providing for specific exceptions from the general data protection framework under the Act.[7] Specific provisions that differ from the general rules of the Act are contained within the Labor Code.[8] According to the Office, based on the decision of the European Court of Human Rights, employees may legitimately expect their privacy protection rights to be recognized even at the workplace and the employer shall respect these rights.[9]

As of 1 May 2004, the Czech Republic is a Member State of the European Union (EU) and has implemented into the Act all remaining provisions of the Directive, in particular those related to the free movement of data within the EU and restrictions on the transfer of personal data to third countries. Nevertheless, it must be stressed that the Act goes beyond the harmonized rules in some aspects and provides for much more strict regulation in the area of personal data processing.

1.2. Application of the Act

The Act applies to any personal data processing, both by

---

[3]Section 12 of Act No. 40/1964 Coll., the Civil Code, as amended.

[4]Act No. 127/2005 Coll., on the Electronic Communications and on Amendment to Some Acts, as amended.

[5]Act No. 480/2004 Coll., on the Information Society Services and on Amendment to Some Acts, as amended.

[6]Act No. 133/2000 Coll., on evidence of inhabitants and on birth numbers and on Amendment to Some Acts, as amended.

[7]Act No. 106/1999 Coll., on Free Access to Information, as amended; Act No. 258/2000 Coll., on Public Health Protection and on Amendment to Some Acts, as amended.

[8]Act No. 262/2006 Coll., the Labor Code, as amended.

[9]Niemitz vs. Germany, Halford vs. United Kingdom.

automatic and other means, by state authorities, territorial self-administration bodies, other public authority bodies, as well as by natural persons and legal persons with the following exceptions:

- Personal data processed by natural persons for their own personal needs exclusively; and
- Accidental personal data collection unless these data are subject to further processing.

The Act also applies to personal data processing:

- Even if the data controller is not established in the Czech Republic on the condition that the laws of the Czech Republic are applicable preferentially under the international public law;
- If the data controller who is established outside the territory of the EU carries out processing on the territory of the Czech Republic, which is not limited to personal data transfers across the EU. However, in such a case the data controller is obliged authorize the data processor on the territory of the Czech Republic under the procedure set up in the Act.[10]

If the data controller carries out processing through its organization units established on the territory of the EU, it must ensure that those organization units process personal data in accordance with the national law of the respective Member State of the EU.

2. Legal Definitions

2.1. Personal Data

"Personal data" is defined under the Act[11] as any information that relates to an identified or identifiable natural person. A natural person is considered to be identified or identifiable if it is possible to identify the individual directly or indirectly, in particular on the basis of a number, code, or one or more factors specific to the physical, physiological, psychical, economic, cultural or social identity of the individual.

The scope of data falling under the definition of personal data may vary depending on the actual situation. According

[10]Section 6 of the Act.

[11]Section 4 let. a) of the Act.

to the Czech Personal Data Protection Office (the "Office"),[12] if it is possible to identify a natural person directly or indirectly based on the collected data, such data are considered to be personal data. The so-called identification data, i.e. data that distinguish natural persons, are the most frequent form of personal data. These data are, for example, name and surname, residential address, date of birth or birth registration number. However, if only a name, surname or date of birth is available and a natural person cannot be clearly/directly identified on the basis of this set of data, such data are not considered to be personal data. On the other hand, for example, in the case of processing identification data of a limited group of natural persons—the date of birth or surname could be fully sufficient to clearly and directly identify the natural persons, the data in such case are deemed personal data within the meaning of the Act.

Further, if different pieces of information (e.g., likes, habits, qualities, opinions, various aspects of personality, means, education, profession, etc.) are combined with data that make it possible to identify a natural person, then any such information is considered to be personal data as well. Under the same principle, a computer IP address or Vehicle Information Number may be deemed to be personal data.

Another criterion for determination and/or consideration of data as personal data is the proportionality of time, effort, and material means needed to identify a natural person. If the time, effort, and material means are disproportionate or inadequate, the relevant data cannot be deemed to be personal data.

Certain personal data are considered as especially sensitive and therefore stricter conditions and obligations apply to their processing.[13]

2.2. Personal Data Processing

"Personal data processing" is defined under the Act[14] as any operation or set of operations that is systematically exe-

[12]The Personal Data Protection Office is the supervisory authority for personal data protection in the Czech Republic, which supervises the observance of legally mandated responsibilities in the processing of personal data, maintains a register of instances of notified personal data processing, deals with incentives and complaints from natural persons concerning infringements of the law and provides consultations in the area of personal data protection.

[13]For more details, please see item 4.

[14]Section 4 let. e) of the Act.

cuted by a data controller[15] or a data processor[16] in relation to personal data by automatic or other means. Personal data processing includes, in particular, the data collection, their storage on data carriers, disclosure, modification or alteration, retrieval, use, transfer, dissemination, publishing, preservation, exchange, sorting or combination, blocking and liquidation.

2.3. Transfer of Personal Data

The Act does not expressly define what constitutes a "transfer" of personal data. However, according to the Office, any factual access or disclosure of personal data constitutes a transfer under the Act. Therefore, it is not relevant whether it takes the form of a factual geographical transfer across the state borders, or just viewing the data from another country, for example, via the company's intranet.

3. Personal Data Processing Conditions

3.1. General

Under the Act, the controller of personal data is obliged to:

- Specify the purposes for which personal data are to be processed and process them only in accordance with the purpose for which the data are collected;
- Specify the means and manner of personal data processing;
- Process only accurate personal data and provide all the recipients with the information about blocking, correction, supplementing or liquidation of personal data without undue delay;
- Collect personal data corresponding exclusively to the specified purpose and in the extent that is necessary for fulfillment of the specified purpose;
- Preserve personal data only for the period of time necessary for the purpose of their processing;
- Ensure that personal data obtained for different purposes are not grouped together.

3.2. Consent

Personal data may be processed (and transferred) only

[15]Under Section 4 let. j) of the Act, a "data controller" is someone that determines the purpose and means of personal data processing, carries out such processing and is responsible for such processing.

[16]Under Section 4 let. k) of the Act, a "data processor" is someone that processes personal data on the basis of a special law or authorization by a controller.

with the consent of the natural person concerned (customers, employees etc.). The controller of personal data is entitled to process personal data without the consent of the natural person concerned only if:

- Carrying out processing essential for compliance with the legal obligations of the controller;
- The processing is essential for fulfilling a contract to which the natural person is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the natural person;
- It is essential for the protection of vitally important interests (for example a medical emergency) of the natural person (this provision applies when the natural person's vital interests are threatened and it is not possible to obtain the natural person's consent either because the threat is imminent or because the natural person is not available; in this case, however, the consent must be obtained without undue delay; if the consent is not granted, the controller must terminate the processing and liquidate the data);
- It is in relation to personal data that have been lawfully published in accordance with special legislation (however, this shall not prejudice the right to the protection of private and personal life of the natural person);
- It is essential for the protection of rights and legitimate interests (for example security, property, goodwill etc.) of the controller, recipient or other person concerned (however, such personal data processing may not conflict with the right of the natural person to protection of his/her private and personal life);
- The controller provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity, their function or working position; or
- The processing relates exclusively to archival purposes pursuant to a special act.

The consent of natural person to data processing under the Act must be a free and informed manifestation of will of the natural person the content of which is his/her assent to personal data processing (and transferring). The existence of the natural person's consent is the main pre-condition for personal data processing, *i.e.* personal data processing in the Czech Republic is based on the "opt-in" method. However, the "opt-in" method does not apply for personal data processing for the purpose of offering business opportunities or ser-

vices to the natural person in cases where the natural person's name, surname and address is used for this purpose, provided the data was acquired from a public register or in relation to the activity of data processor or data controller; in this specific case the "opt-out" method applies. This mean that the data specified above may not be further processed if the natural person expresses his/her disagreement therewith. The disagreement with processing must be expressed in writing. No additional personal data may be attached to the data specified above without consent of the data subject. To eliminate the possibility that the name, surname and address of the natural person are repeatedly used for offering commercial services, the data controller is entitled to further process the natural person's name, surname and address for this purpose, despite the fact the data subject expressed his/her disagreement therewith.

The general civil-law rules require that in order for the consent to be valid:

- It has to be made freely, seriously, be comprehensible, and definitive; and
- The natural person, when granting consent, has to have the legal capacity to grant it and must not be acting under mental disorder that would render such consent invalid.

When granting the consent, the natural person must be provided with the information on the purpose of personal data processing, the scope of data processed, to whom the data may be disclosed and on the duration of data processing, unless the data subject is already aware of this information.[17] Although the consent does not have to be granted in a written form, the controller must be able to prove the existence of the consent to personal data processing during the whole period of data processing. Consequently a storable form (in writing, signed, electronically, audio recorded etc.) of the consent to data processing is highly recommended. However, a tick box or double click is considered to be fully sufficient as well.

In the case of sensitive personal data, the consent for their processing must be granted explicitly, i.e. orally or in writing, demonstrating clearly that the natural person agreed to the processing of his/her sensitive personal data.

Pursuant to the general civil-law rules the consent has to

[17]For more details regarding the information duty, please see item 3.3.

be made freely, seriously, be comprehensible, and definitive and, therefore, its withdrawal cannot be always possible and all the relevant circumstances in each and every case of the withdrawal must be properly assessed and evaluated.

3.3. Information Duty

The controller is obliged to inform the natural person in advance on the scope and purpose for which the personal data shall be processed, who shall process the personal data and in what manner and to whom the personal data may be disclosed, unless the data subject is already aware of this information.

The controller must further inform the natural person of his or her right of access to personal data, the right to have his/her personal data rectified as well as the rights to know information about his/her personal data kept by the controller and to ask for explanations and removal of a detrimental situation. This information has to be provided at the latest when personal data are collected.

In cases when the controller processes personal data obtained from the natural person, it must instruct the natural person on whether the provision of personal data is obligatory or voluntary. If a natural person is obliged pursuant to a special law to provide personal data for the processing, the controller must instruct him/her on this fact as well as on the consequences of refusal to provide the personal data.

The controller need not provide information if:

- The natural persons are already aware of the information;
- The controller did not obtain the personal data from the natural person and is processing personal data exclusively for the purpose of the state statistical service, scientific or archival purposes, and the provision of such information would involve a disproportionate effort or inadequately high costs;
- The controller must meet legal obligations arising from a special act or when such personal data are necessary to exercise its rights and obligations following from a special act;
- It has been lawfully published; or
- It was originally obtained with the natural person's consent.

Furthermore, the controller does not have this obligation if the personal data are not obtained from the data subject, and if the processing of personal data is necessary to ensure

(a) the security of the Czech Republic, (b) the defense of the Czech Republic, (c) public order and internal security, (d) the prevention, investigation, detection and prosecution of criminal offences, (e) important economic or financial interests of the Czech Republic or of the European Union, (f) activities related to any disclosure of the former State Security files, or (g) control, supervision, surveillance and regulation related to cases under (c), (d) and (e).

The Act contains no strict conditions and/or obligations with regards to how the information should be provided or communicated to the natural person. Nevertheless, information has to be provided in such a way that there is a reasonable level of probability that it actually reaches the natural person. The meeting of this obligation is assessed based on the proportionality. In other words, if the controller is addressing a large number of natural persons and he has made a reasonable effort to provide the information to them, the obligation shall be deemed to have been fulfilled. This occurs, for example, if a company with more than one million customers provides information to them via media in visible ways, such as advertisement in several national newspapers and through publication on the Internet. Publishing of information on the Internet is sufficient if the concerned natural persons are made aware of it, for example, when entering into the contract etc. This information need not be provided in writing.

3.4. Security Requirements

The controller and the processor must adopt measures preventing unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transmission, other unauthorized processing, as well as other misuse of personal data. In the framework of these measures, the controller or the processor perform a risk assessment concerning the carrying out of instructions for personal data processing by persons who have immediate access to the personal data, prevention of unauthorized persons' access to personal data and means for their processing, prevention of unauthorized reading, creating, copying, transferring, modifying or deleting of records containing personal data, and measures enabling to determine and verify to whom the personal data were transferred. In the area of automatic processing of personal data, the controller or processor shall be obliged to ensure that the systems for automatic processing of personal data are used only by authorized persons, that the natural persons authorized to use systems for

automatic processing of personal data have access only to the personal data corresponding to their authorization and on the basis of specific user authorizations established exclusively for these persons, that electronics are made enabling to identify and verify when, by whom and for what reason the personal data were recorded or otherwise processed, and to prevent any unauthorized access by data carriers.

In addition, the controller or the processor must develop and document technical-organizational measures adopted and implemented to ensure the protection of personal data protection in accordance with legal regulations.

The above-cited obligations are usually met by implementation of a security directive (in the case of large databases, only after the security audit is performed), which demonstrates and describes the particular security measures adopted by the controller or processor. The scope of the security directive depends on the actual number and scope of data processed.

The Office's notification form that the controller has to complete gives some examples of such measures and requires the controller to indicate whether he or she has implemented any of these measures. The listed measures include locks, bars, electronic security, centralized security switchboard, internal security directives/policies, other documentation released to the implemented technical-organizational measures, access rights and virus protection, security backups or encryption.

3.5. Notification to the Office

Under the Act,[18] whoever intends to process personal data as a data controller, including transferring data internationally is obliged to notify such intention in writing to the Office. Should a legal person established outside the Czech Republic perform personal data processing in the Czech Republic through a data processor, such processing still has to be registered with the Office; in such case the processor on the Czech territory shall notify the Office of the intended data processing.

The notification must include the following information:

- The identification data of the controller;
- The purpose or purposes of processing;
- The categories of natural persons and of personal data pertaining to these natural persons;

[18]Section 16 (1) of the Act.

- The sources of personal data;
- The description of the manner of personal data processing;
- The location or locations of personal data processing;
- The recipient or category of recipients;
- The anticipated personal data transfers to other countries;
- The description of measures adopted for ensuring the protection of personal data.

The notification can be submitted to the Office either electronically or in writing using either the special registration form published by the Office on its website or a notification letter containing all statutory information pursuant to the Act.

If the notification includes all essentials, the personal data processing may commence after a lapse of 30 days following the delivery of the notification to the Office. If the notification does not include all essentials, the Office will send without delay a request to the applicant for supplementation and set a deadline for supplementing the notification. If the Office does not receive the notification supplement within the set deadline, the notification shall be regarded as if it has not been submitted.

In the case of a successful notification, the Office records the information stated in the notification into the register. The register kept by the Office is available on the Office web site.[19] It is possible to search in the register by the name of the subject, the allocated registration number or the company identification number.

The notification obligation does not apply to processing of personal data:

- That are part of data files publicly accessible on the basis of a special act,
- That are 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, or
- In case of processing that pursues political, philosophical, religious or trade-union aims carried out within the scope of legitimate activity of an association and which relate only to members of the association or persons with whom the association is in recurrent contact and relating to legitimate activity of the association, and

[19] http://www.uoou.cz.

the personal data are not disclosed without the consent of the data subject.

Nevertheless, the controller who carries out processing not subject to the notification duty is required to ensure that the information concerning in particular the purpose of the processing, categories of personal data, categories of data subjects, categories of recipients and the period of preservation, which would otherwise be accessible by means of the register maintained by the Office, is disclosed to the concerned natural persons through remote access or in another appropriate manner.

4. Sensitive Data

"Sensitive data" is defined under the Act[20] as data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, criminal conviction, health status, sexual life as well as any genetic data and biometric data that enable the identification or authentication of the data subject directly (fingerprint, retina image etc.).

Sensitive data may be processed only with the natural person's explicit consent. Without such consent, the sensitive data may only be processed in specific situations such as when required by a special act or to preserve someone's life or health.

Sensitive data may be processed on the following conditions:

- The data subject expressly consents;
- The consent cannot be obtained but the processing is required in order to preserve the life or health of the data subject or another person or to eliminate imminent serious danger to their property;
- The processing is required to ensure health care, public health protection, health insurance, and the exercise of public administration in the field of health sector, or it is related to the assessment of health in other cases;
- The processing is required for the controller's compliance with labor law and employment rights and duties;
- The processing pursues political, philosophical, religious, or trade-union aims, is performed within the scope of a non-profit entity's legitimate activities, and relates only to members or affiliated persons of that entity, and provided that the personal data are not made accessible without the data subject's consent;

[20]Section 4 let. b) of the Act.

- The data are required by the law for health insurance, social insurance, state social support, and other state social benefits, social care, and social and legal protection of children;
- The processing concerns personal data published by the data subject;
- The processing is necessary to secure and exercise legal claims;
- The data are processed exclusively for archival purposes; or
- The processing is performed under special acts with regard to crime prevention, inspection, detection, prosecution, and search for persons.

All the above-listed exceptions apply to all types of categories of sensitive data. The Office does not distinguish specific exceptions for various types of sensitive data.

5. International Transfer

5.1. Transfer to Member States of the EU

According to the Act,[21] the personal data may be transferred to other Member States of the EU[22] without any restrictions.

However, personal data transfers have to meet the requirements set forth by the Act for personal data processing as stated above, including notification of the intended transfer to the Office pursuant to which the information will be entered into the register kept by the Office.[23] In particular, if the data controller uses a data processor, the parties should always enter into a controller-processor agreement, even if the data processor is established in another Member State of the EU. On the other hand, if a Czech entity or a natural person collects and processes personal data in the Czech Republic for a data controller based in another Member State of the EU on the basis of a special agreement, such entity or natural person will be in the position of a data controller from the viewpoint of the Act, even if the purpose of personal data processing is determined by another person, i.e. by the

[21]Section 27 (1) of the Act.

[22]Currently the Member States of the EU are as follows: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

[23]For the register kept by the Office, please see item 3.5.

original data controller. This is why the personal data processing in the Czech Republic through a data processor has to be registered with the Office.

5.2. Transfer to Non-EU Countries

5.2.1. Third Countries that Provide for an Adequate Level of Protection

According to the Act,[24] the personal data may be transferred to third countries, i.e. outside the EU, only with the Office's authorization (i.e. special approval), unless the third country provides for an adequate level of protection of personal data. In theses cases, the personal data transfers have to meet the Act's requirements for personal data processing as stated above, including notification of the intended transfer to the Office.[25] In other words, the rules applicable to personal data processing in the Czech Republic require the personal data transfers to be subject to these rules even if transferred abroad.

The first group of countries considered as safe (adequate) in terms of personal data protection are countries that have ratified an international treaty binding the Czech Republic and prohibit the restriction of free movement of personal data and whose legislation thus guarantee sufficient protection of personal data in keeping with all requirements of the Directive and of the Act as well. The second group of countries considered as safe (adequate) consists of countries to which personal data are transferred on the basis of a decision of an institution of the EU. The Office publishes information about such decisions in the Official Journal.

5.2.2. Third Countries that Do Not Guarantee an Adequate Level of Protection

The personal data transfer to countries that do not guarantee an adequate level of protection is allowed subject to the Office's authorization (i.e. special approval) and if one of the following conditions is met:

- The natural person consents to or instructs the transfer;
- The destination country provides adequate special guarantees for the personal data protection (such guarantees may be specified in a contract between the controller and the recipient, e.g. if the contract contains contractual clauses for personal data transfers to third countries published in the Official Journal of the Office);

[24]Section 27 (2) of the Act.

[25]For more details, please see item 3.5.

- A special Czech law or international treaty binding the Czech Republic allows it either with regard to certain publicly accessible data files or due to important public interest;
- It is required in order to perform an agreement between the data subject and a third party or for negotiations about entering into or changing an agreement initiated by the data subject;
- It is required in order to perform an agreement entered into between the data controller and a third party in the data subject's interest; or
- It is required to protect the data subject's rights or vital interests.

The application for granting an authorization (i.e. special approval) is processed by the Office pursuant to the special act[26] within 30 days or within 60 days if the case is more difficult. In assessing the application, the Office examines all circumstances related to the personal data transfer, in particular the source, final destination and categories of personal data to be transferred, the purpose and period of the processing, with regard to available information about legal or other regulations governing the personal data processing in a third country.

If the information contained in the application is insufficient for the evaluation of the transfer of personal data and the issuance of its authorization, the Office may suspend the proceeding and request the additional submission of any such missing information, including any relevant evidence. In the authorization, the Office specifies the period in which the controller may perform the personal data transfers. If the conditions under which an authorization has been issued should change, the Office may alter or revoke its authorization.

6. Overcoming the Restrictions on International Data Transfers

6.1. International Treaty

Personal data transfers are allowed without the Office's authorization (*i.e.* special approval) to third countries that have ratified the Convention for the protection of natural persons with regard to automatic processing of personal data (Council of Europe, ETS 108, 1981) and whose legislations thus guarantee sufficient protection in keeping with all

[26] Act No. 500/2004 Coll., the Administrative Code, as amended.

requirements of the Directive (and thus also of the Act).[27] However, any such intended transfer of personal data must be duly notified to the Office in advance.[28]

6.2. EU Institution Decisions

Under the Act, personal data may be transferred without the Office's authorization (*i.e.* special approval) to third countries that the Commission of the European Union (the "Commission") has specifically determined as providing adequate protection for personal data pursuant to the Directive (and thus also to the Act).[29] However, any such intended transfer of personal data must be duly notified to the Office in advance.[30]

6.3. Standard Contractual Clauses

Personal data transfers are allowed without the Office's authorization (*i.e.* special approval) to third countries if the personal data "exporter" based in the Czech Republic and the personal data receiver based in a third country enter into a contract based on the standard contractual clauses ("Model Clauses") worded exactly as provided in the Commission's decisions. However, any such intended transfer of personal data must be duly notified to the Office in advance.[31] If the wording differs in any way from the Model Clauses, it will be necessary to obtain the Office's authorization (*i.e.* special approval) in advance so that it can review the adequacy of such contractual arrangements.

The Commission has issued three decisions so far that include Model Clauses.[32] One set of Model Clauses consisting of the old and the new clauses that can be used to transfer

---

[27]Currently the following countries fall under this category: Albania, Andorra, Bosnia and Herzegovina, Croatia, Georgia, Iceland, Liechtenstein, Macedonia, Moldavia, Montenegro, Norway, Serbia and Switzerland.

[28]For more details, please see item 3.5.

[29]Currently the following countries fall under this category: Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Jersey and Switzerland. However, in case of Canada it is advisable to consult the Office.

[30]For more details, please see item 3.5.

[31]For more details, please see item 3.5.

[32]Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (2001/497/EC); Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (2002/16/EC); Commission Decision of 27 December 2004, amending Decision 2001/

data outside the EU and is intended for the so-called controller-to-controller relationships, *i.e.* relationship between a local data controller and a data controller established outside the EU. Both the old and the new data controller-to-controller Model Clauses can be used to transfer data outside the EU. However, the new clauses provide a lighter liability regime and are more flexible.

The second set of Model Clauses is intended for the so-called controller-to-processor relationships, *i.e.* relationship between a local data controller and a data processor established outside the EU (such as an external IT-service provider or an outsourcing company that is used by the data controller to process the personal data). The controller-to-processor Model Clauses are less extensive than the controller-to-controller Model Clauses, which counteract the risks brought about by the independent decision-making powers of the data controller established outside the EU. Currently, the Commission is in the process of updating the controller-to-processor Model Clauses to better accommodate the needs of corporations that have an outsourcing company.

6.4. Ad hoc Contract Clauses

Furthermore, personal data transfers are allowed to countries, which do not guarantee an adequate level of protection if a contract concluded between the controller and the recipient contains contractual clauses for personal data transfer to third countries published in the Office Journal of the Office. However, such transfers require the Office's prior authorization in advance (*i.e.* special approval).

6.5. Safe Harbor

Personal data transfers to third countries are allowed without the Office's authorization (*i.e.* special approval) if the receiving party is a Safe Harbor member, but in these cases it is advisable to consult the Office. The Safe Harbor is an initiative developed by US authorities in order to comply with EU personal data transfer regulation following the Commission's determination that the laws of the USA do not adequately protect personal data. A company that enters the Safe Harbor has to meet the personal data protection criteria required by the EU Data Protection Directive.

6.6. Binding Corporate Rules

Personal data can be transferred to third countries if the

497/EC, as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC).

destination country provides adequate "special" guarantees for the personal data protection. Such "special" guarantees can be achieved by the adoption of binding codes of corporate conduct based on Art. 26 (2) of the Directive, known as Binding Corporate Rules (BCR).

BCRs are an internal set of rules adopted within a particular company or corporate group that provide legally-binding protections for data processing within the company group enforceable by third parties. BCRs are legally binding on members of a corporate group but do not apply to transfers to those outside the corporate group (for example to an outsourcing company). For these so called onward transfers, the data controller must ensure an adequate level of privacy protection as required under Czech law (for example based on the standard contractual clauses), which is why BCRs are unlikely to be used extensively.

As in other EU Member States, BCRs must be notified to, and be approved by, the Office. Since BCRs are approved on a national level in each country in which the group is located, the approval process in many countries may be the main obstacle to use the BCRs. So far the Office has never been the leading authority within the approval process and it has not agreed to mutual recognition of BCRs approved by other protection authorities without any further amendments.

6.7. Important Public Interest

Under the Act, personal data can be transferred outside the EU only with the Office's prior authorization (*i.e.* special approval) if it is necessary to exercise an important public interest arising from a special Czech law or from an international treaty binding the Czech Republic. The Office applies a rather narrow interpretation of important public interest and the individual's privacy right, giving more weight to the individual's privacy rights. Before relying on important public interests, it should always be assessed whether the same result can be achieved with fewer data or by less invasive means and whether and to what extent the processing would affect an individual's privacy.

6.8. Vital Interests

Under the Act, personal data can be transferred outside the EU only with the Office's prior authorization (*i.e.* special approval) if the transfer is necessary for the protection of rights or important vital interests of the data subject, in particular for rescuing life or providing health care.

6.9. Transfers from a Public Register

Under the Act, personal data can be further transferred outside the EU only with the Office's prior authorization (*i.e.* special approval) if the personal data concerned are part of statutory publicly accessible registers or are accessible on statutory grounds to someone who is able to prove a legal interest. In such a case, however, the personal data may be disclosed only in the scope and under conditions provided by a special act. Examples of these registers are, for example, the commercial register, the trade register, the real estate register, registers of professional chambers (such as public notary register, attorney-at-law register) etc.

6.10. Contractual Necessity

Finally, under the Act, personal data can be transferred outside the EU only with the Office's prior authorization (*i.e.* special approval) if the transfer is necessary:

- To perform an agreement between the data subject and a third party;
- To negotiate on entering into or changing an agreement initiated by the data subject; or
- To perform an agreement entered into between the data controller and a third party in the data subject's interest.

The key ground to this legal basis for transferring data is the necessity requirement. Generally, it is important that unnecessary personal data are not processed and transferred.

7. Consequences of Noncompliance

In the Czech Republic there are three main consequences of noncompliance with the rules applicable to personal data processing, including international transfers of personal data. These are criminal sanctions in serious cases, administrative sanctions under the Act and civil sanctions under the Civil Code,[33] which can be initiated by a natural person that was harmed by the misconduct.

7.1. Criminal Sanction

Czech law recognizes criminal sanctions for severe violation of personal data protection even if the conduct is negligent.

A person who:

- Without authorization discloses, processes, or acquires

[33] Act No. 40/1964 Coll., the Civil Code, as amended.

personal data of another person that was collected in relation to public administration,

- In relation to their work position or other position violate the statutory obligation of confidentiality by disclosing the personal data of another person,

commits a crime of unauthorized use of personal data. The sanction is up to 5 years of imprisonment in the most severe cases.

7.2. Administrative Sanction

7.2.1. Measures of remedy

If a data subject presumes that the controller is processing data in conflict with the law or the data subject's rights to protection (in particular if the personal data are inaccurate with regard to the purpose of their processing), the data subject may (a) seek a remedy against the controller, or (b) appeal directly to the Office.

When seeking remedy from the controller, the data subject may (a) ask the controller for explanation, or (b) request the controller to remedy the situation. If the data subject's requirement is found justified, the controller is required to remove any defects immediately. If the controller fails to satisfy the data subject's requirement, the data subject may appeal to the Office. There is no strict timeframe for evaluating whether the data subject's requirement is justified, but it is advisable to perform the evaluation without undue delay.

Upon finding a breach of obligation of the Act, the Office may determine remedial measures to be adopted in order to eliminate the established shortcomings and set a deadline for their elimination by the data controller or any other entity or natural person processing personal data. These measures are not explicitly listed in the Act and depend on the nature of the breach. However, an example of these measures of remedy would be blocking, correcting, supplementing, erasing or liquidation of unlawfully processed personal data. If deletion of personal data has been ordered, the relevant personal data shall be blocked until their deletion.

7.2.2. Fines

In addition, noncompliance with the Act may result in fines of up to CZK 5,000,000 (approx. EUR 180,000) if the violation was committed by a natural person or up to CZK 10,000,000 (approx. EUR 360,000) if the violation was committed by an entity. When deciding about the amount of the fine in the event of a violation, the following is taken into ac-

count especially: severity, manner, duration, consequences of the violation, and circumstances under which the violation was committed.

If the violator is an entity, it is not liable for the breach of a legal obligation, if it proves that all efforts that could reasonably have been required were taken to prevent a violation of a legal obligation. Liability of an entity for violation of the Act is extinguished if the Office does not initiate proceedings within one (1) year from learning about the violation, but no later than within three (3) years from the day on which the violation was committed.

The Office imposes penalties effectively and is known for its strict approach to enforcement of the data protection rules. Where serious breaches and high fines are involved, the public usually gets the information from media and even image damage may be caused. However, the Office has neither penalized nor dealt with international data transfer by companies nor prevented personal data transfers (including viewing) so far.

7.3. Civil Sanction

If the data controller or any other entity or natural person processing personal data violates the data subject's privacy, the data subject can, regardless of any fines that the Office imposed, file a civil action requesting the court in particular to

- Bar the person or entity from continuing the misconduct;
- Order to reinstate matters, if possible;
- Order to provide reasonable satisfaction (typically an apology) to the data subject, which can be rendered in money; and/or
- Order to pay damages to the data subject.

8. Future Trends

We expect that the Office—also in cooperation with the personal data authorities in other EU countries—will develop and define in a more precise manner the rules and conditions for crossborder flow of personal data reflecting the actual technology developments and the justified needs and interests of the business and natural persons.