Education and Culture DG
Lifelong Learning Programme
Leonardo da Vinci

Selected data protection issues

Guide for entrepreneurs

úřad pro ochranu osobních údajů
the office for personal data protection

HUNGARIAN PARLAMENTARY COMMISSIONER FOR
DATA PROTECTION AND FREEDOM OF INFORMATION

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Education and Culture DG
Lifelong Learning Programme
Leonardo da Vinci

This publication was developed as a result of the Leonardo da Vinci Partnership Project “Raising awareness of the data protection issues among the entrepreneurs operating in the EU”. The project has been funded with support from the European Commission under the Lifelong Learning Programme.

The guide “Selected data protection issues. Guide for entrepreneurs” is the result of an international cooperation of experts representing three Data Protection Authorities:

- Bureau of the Inspector General for Personal Data Protection in Poland
- Office for Personal Data Protection in the Czech Republic
- Data Protection and Freedom of Information Commissioner in Hungary

For non-commercial purposes, a download version of this publication is available at the websites of the partners’ Data Protection Authorities.

úřad pro ochranu osobních údajů
the office for personal data protection

HUNGARIAN PARLAMENTARY COMMISSIONER FOR
DATA PROTECTION AND FREEDOM OF INFORMATION

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Foreword

The twenty-first century is often referred to as the information age. It is an idea that human activity depends on the exchange of information. Modern technology enables us to gather, evaluate, transfer, and process unprecedented quantities of data. People now have instant access to information that was not available previously. With this ability, the risk of misusing people's privacy and its unwanted consequences grows proportionally. Data protection plays an important part in ensuring that people have confidence in information technology.

The purpose of this publication is to inform entrepreneurs and employees about data protection. This guide explains how an adequate system of data protection helps develop the corporate culture of social responsibility. Moreover, it raises the awareness that data protection can be a great competitive advantage especially for some types of businesses. This booklet will acquaint you with the basic data protection principles and your legal obligations in this area.

We believe this guide will become a valuable help for you.

1. Introduction

Starting a business activity, in particular in another country requires familiarisation with a variety of legal provisions, which have a significant impact on the day-to-day activity of entrepreneurs. These include, among other things, provisions on taxation, labour law, consumer law as well as legislation on the protection of personal data and privacy.

Business activity is related to the need to use personal data, hence every entrepreneur commencing his or her activity in the Czech Republic, Hungary or Poland needs to fulfil obligations in the field of data protection. Such obligations apply to sole traders and to large commercial companies alike.
The present guide outlining the general issues concerning data protection is addressed to entrepreneurs who want to start and operate in foreign markets: the Czech Republic, Hungary and Poland.

A general overview of the Czech, Hungarian and Polish national laws on the protecting of data is presented below. However, in order to obtain detailed information, we recommend that you contact the data protection authority in a given EU Member State and get acquainted with the materials placed on its website.

2. European and national legislation and basic definitions of data protection

2.1 The European and national laws on data protection

In Europe, the protection of personal data is of special importance. As one of the fundamental rights, it is guaranteed by a number of international and national legal acts. The right to respect for private and family life is guaranteed under Article 8 of the European Convention on Human Rights. The first international legal act to regulate this issues in a comprehensive manner is the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe on January 28, 1981. At the European Union level, the principal legal act is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Moreover, the right to personal data protection is also safeguarded as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union and in Article 16 of the Treaty on the Functioning of the European Union. In the EU law, in addition to Directive 95/46/EC, other legal acts regulate the issue of personal data protection. To a large extent, they complement the provisions of Directive 95/46/EC, which is general in nature and serves as a point of reference for the relevant legislation of the EU countries.

The Directive 95/46/EC regulates the right to protection of privacy of each natural person with respect to the processing of personal data, which is one of the fundamental rights and freedoms of natural persons. The Directive is applied to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

More information – see
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

The principal objective of Directive 95/46/EC is to ensure the highest possible level of personal data protection and to facilitate free movement of data within the European Union and in practice within the entire European Economic Area.

The collection and use of personal data in the Community must be carried out in accordance with the law of the Member State, in which the business of a controller responsible for the processing of such data is established. If an organisation is established in several Member States, for example by means of subsidiaries, the handling of personal data by each subsidiary must comply with the data protection law of the Member State in which the subsidiary is based.

EU Member States were obliged to implement the provisions of the Directive into their legal systems. Member States were given a certain margin of discretion in its implementation leading to potential differences in national legislations. Entrepreneurs doing business in these countries should be aware of this fact. This publication identifies such differences in the Polish, Czech, and Hungarian laws.

Polish legislation

In Poland, the right to privacy and data protection is guaranteed in the Constitution of the Republic of Poland (cf. Article 47 and Article 51, respectively). The principles of data processing and the rights of natural persons whose personal data are or may be processed in data filing systems are specified in the Act on the Protection of Personal Data of 29 August 1997 (restated text: Journal of Laws of 2002 No. 101 item 926 with amendments, hereinafter referred to as the Act) and in secondary legislation adopted on its basis: the Regulations of the Minister of Interior and Administration:

1. The Regulation of 29 April 2004 on personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for personal data processing (Journal of Laws No. 100 item 1024) – adopted on the basis of Article 39a of the Act – specifies:
   - the type and the scope of documentation describing the way data are processed and the technical and organisational means ensuring the protection of the processed data – commensurate with the risks and with the category of protected data;
   - the main technical and organisational requirements to be fulfilled by IT systems and devices used to process personal data;
   - the requirements applied to recording of data disclosure and to the security of data processing.
2. The Regulation of 11 December 2008 on specimen of notification of a data filing system for registration by the Inspector General for Personal Data Protection (Journal of Laws No. 229 item 1536) – adopted on the basis of Article 46a of the Act – specifies the specimen of notification, constituting appendix thereto.
3. The Regulation of 22 April 2004 of the Minister of Interior and Administration on the specimen of personal authorisations and service identity cards of the inspectors employed in the Bureau of the Inspector General for Personal Data Protection (Journal of Laws No. 94 item 923) – adopted on the basis of Article 22a of the Act – specifies the specimen.

The data protection system also comprises other specific provisions, e.g. provisions of the Civil Code on the protection of personal interests and other provisions regulating the use of personal data.

In Poland, the authority responsible for oversight of compliance of data processing with the provisions on the protection of personal data is the Inspector General for Personal Data Protection (http://giodo.gov.pl/).

Czech legislation

The main law regulating personal data protection in the Czech Republic is the Act No. 101/2000 Coll., on the protection of personal data and on amendment to some acts (hereinafter referred to as “Act 101”) which is an integral part of the Czech Republic’s legal system in a dual way:

- It is related to Articles 10 and 17 of the Charter of fundamental rights and freedoms providing for the right to information on the one side, and establishing the right to privacy protection, on the other side. Thus, Act 101 offers a solution to the contradicting nature of the above mentioned rights. However, it is not the sole regulation of this kind, since the Civil Code (Act No. 40/1964 Coll., as amended) also contains provisions for the protection of personality, which is vitally related to the notions of “personal data processing” and “data subject” as defined by Act 101.
- Act 101 is a general law regulating the processing of personal data in the territory of the

Czech Republic, except for processing done by natural persons for purely personal needs. However, the Act 101 permits processing of personal data for special purposes, (pursuant to Directive 95/46/EC) also in order to fulfil tasks mandated by law. Entrepreneurs have to examine whether the intended or already running processing operation does not fall under a special legal regulation. If this is the case, then the Act 101 would be applicable as secondary law. Otherwise the Act 101 take precedence over other laws.

The Act 101 (and personal data protection law as such) can be divided into three thematic parts:

1. Provisions regulating conditions of personal data processing (contained in Articles 5-19 and Article 27 of the Act 101), laying down the legal groundwork for the processing of personal data (for example, the data subject's consent, the obligation to fulfil a contract, or the execution of tasks mandated by a special law).
2. Provisions regulating the consequences of a breach of data processing principles. It concerns the following items:
   - remedy which can have the form of liquidation of data, termination of unlawful processing, etc. (see Article 40 of the Act 101); a remedy, however, is not the same instrument as a sanction;
   - penalties (see Chapter VII of the Act 101). Criminal law sanctions - unlawful treatment of personal data for instance is a criminal act under Article 180 of the Criminal Code;
   - damages, where provisions of the Civil Code and Commercial Code apply.
3. Procedural provisions setting out methods of the enforceability of rights in the event of a violation of data protection rules. Proceedings in which recourse is made to satisfactory measures must be brought before court; criminal cases must be handled by the law enforcement authorities, and in other instances the competence lies with the OPDP as an independent supervisory authority (Chapter V of the Act 101).

In the Czech Republic, competencies in the field of personal data protection are vested in the Office for Personal Data Protection (http://www.uoou.cz/). Only processing operations conducted by the intelligence services are outside the OPDP's competence. The Office is responsible, among other things, for the handling of complaints about breaches of data protection rules (a complaint or a motion can be lodged, free of charge, and by everyone, even those who are not citizens of the Czech Republic) and offers consultancy without charge.

 Hungarian legislation

In Hungary, the right to the protection of personal data is ensured by the Constitution. The substantial specification of this fundamental right and its scope is regulated by the Act LXIII of 1992 on the protection of personal data and public access to data of public interest (hereinafter referred to as DP & FOI Act). This act transposed the provisions of Directive 95/46/EC into the Hungarian law. Besides the Data Protection Act, several sector-related acts contain significant regulations on data protection. The DP &FOI Act and other sector-related acts have been amended till now.

The main chapters of the DP&FOI Act containing the basic definitions and fundamental data protection rules are modelled on Directive 95/46/EC. The Act specifies the competence and powers of the Data Protection Commissioner and regulates public access to data of public interest, and the use of personal data for research or statistical purposes.

In Hungary, the authority overseeing the law on data protection is an independent authority – the Data Protection and Freedom of Information Commissioner (http://www.adatvedelmibiztos.hu/abi/).

2.2 The definitions related to data protection law

Definitions related to the data protection law are based on Article 2 of Directive 95/46/EC.

Personal data and data subject

Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The notion of personal data is of vital importance, because data protection acts apply solely to information constituting personal data. The protection of other information may be guaranteed by other provisions.
Personal data constitute a set of data items which allows a person to be identified to such extent that it is possible to distinguish that data subject from other data subjects and to contact him/her or to make it relatively easy to establish contact with him/her, and to make conclusions with respect to a data subject which can be inferred from such data. In the course of data processing such data shall be considered personal as long as their relation to the data subject can be restored. Information related to legal persons or organisational units without legal personality is not considered personal data. Also information about a deceased person is not classified as personal data, unless in a particular situation this information concerns persons who are alive. Entrepreneurs most often use basic information about natural persons, like names, surnames, addresses, dates of birth, identification numbers or other most frequently used data, disclosed in everyday situations. The legislation on personal data protection does not include a complete catalogue of data categories, because due to the complexity of the notion of personal data, it would be impossible to create such catalogue.

There are no specific national variations.

There are no specific national variations.

In Hungary, the personal data of persons managing a legal entity (e.g. the managing director or acting partner) included in the Company Registry are public pursuant to the Act V of 2006 on Public Company Information, Company Registration and Winding-up Proceedings. This public registry contains personal data, for instance, the name, date and place of birth, maiden name of the mother of chief executive officers or managers.

Sensitive data

Sensitive data shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Data related to offences, convictions or security measures, data concerning administrative sanctions or judgments in civil cases may have a similar status.

Pursuant to Directive 95/46/EC, the acts of particular Member States comprise a self-contained catalogue of special categories of data, the so-called sensitive data. Given their nature, sensitive data have been singled out under a special protection regime, because they may cause flagrant violations of individual rights and freedoms, e.g. discrimination.
It should be borne in mind that the catalogues of sensitive data may differ from country to country.

The notion of personal data does not cover information on entrepreneurs, including natural persons conducting activity as sole traders, insofar such information identifies them in trading and they are entered into the register of business activity.
In the Polish Act, the catalogue of sensitive data is more precise and covers information on political parties' membership, genetic code, addictions, convictions, decisions imposing penalty, fines and other decisions issued in court or administrative proceedings.

Data on natural persons doing business are also understood as personal data. The use of birth dates is strictly restricted under the Act No.133/2000 Coll.
Sensitive data also include data that reveals ethnicity, data on conviction for a criminal act, and genetic and biometric data, if they enable direct identification or authentication of a data subject. In applying the Act, consider the following:

1. Data on ethnicity has to be clearly distinguished from data on citizenship. These notions are often mistaken in the colloquial language.
2. Information on political party membership is regarded as sensitive data revealing political opinions or standings. However, the Constitutional Court has ruled that information on membership of the Communist Party before 1989 is not sensitive.
3. Information on convictions for a criminal act is regarded as sensitive. As such, it cannot be regarded as information on a conduct that could be classified as criminal, or data on other sanctions, e.g. fines. However, information that a particular person has not been convicted for a criminal offence, for instance a clean criminal record extracted from the crime register is not considered sensitive data. Neither is information about a certain conduct that meets the characteristic of a criminal act that went unpunished on the grounds of the offender's minor age, for instance.
4. Biometric data can be generally understood as data about measurable or objectively classifiable parameters of the human body. The Act 101, however, adds one other criterion-that of the possibility of directly identifying or authenticating someone. So, in broader terms, the length of a person's foot is not considered biometric data, but a his fingerprint is.

Data on natural persons running a business are also considered personal data. The concept of sensitive data also includes information about the data subject's membership in any interest representing / representative / advocacy organization as well - which is very important - in the field of labour law and employment. The legislator also widened the scope of sensitive data in the concept of criminal personal data. It means any personal data which originated – during criminal proceedings or prior to such proceedings in connection with the criminal offence or the criminal proceedings – from bodies authorised to conduct criminal proceedings or to investigate criminal offences or from the penal authorities and which can be related to the data subject, as well as personal data concerning previous criminal convictions.

Processing of personal data

Processing of personal data ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

This notion is very important for entrepreneurs, because they need a proper legal basis for each operation of personal data processing.
The processing may be carried out once or several times, may be identical or compatible technologically. It is very important to remember, that a single (one-time) operation upon data, e.g. their disclosure, shall be treated as their processing.
The most common operations considered as data processing are photographing, sound or image recording, as well as the recording of physical characteristics suitable for personal identification (such as fingerprints, and palm prints, DNA samples and iris images). The storage of data is also regarded as data processing.

There are no specific national variations.

Processing is understood as an operation or set of operations that are executed systematically. Consequently, solely a particular kind of operation that is performed repeatedly and the realization of which is technologically identical or compatible is understood as processing. It cannot be ruled out that a set of operations will occur only once. Or, one single operation out of the whole set takes place. What determines its nature is the intention to repeat or pursue these operations under given circumstances. This intention can be documented in the form of workflow descriptions, technical or software elements, etc. The term "personal data processing" could for instance be synonymous with "keeping a certain register, file, or catalogue". One-time treatment of personal data (single publication or communication) does not fall under the scope of the Act 101.

Any operation upon data, even a single (one-time) operation, e.g. their disclosure, shall be treated as their processing.
Technical data processing is a specific form of processing. It consists of performing technical tasks related to data processing operations, regardless of the methods or means employed or the place of application.

Personal data filing system

Personal data filing system ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

The possibility to search according to any personal criterion (name, surname, date of birth, identification number) or non-personal criterion (data entry date in the filing system) determines the organised nature of a set of data and thus allows to classify such set as a data filing system.
A typical data filing system in the case of entrepreneurs are, to give an example, personal records of employees collected in relation to their employment and the work performed by them, or consumer files. The files may be kept both in IT systems and in paper form.

Controller

Controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

A controller (often also known as "data controller") decides about the purposes and means of data processing. The controller is responsible for the processing of personal data and for control over such processing. Controllers may include public authorities, local government authorities, economic entities or natural persons conducting economic activity, if they decide about the purposes and means of data processing.

The controller is any natural or legal person or any organisation without legal personality.

The controller is any natural or legal person that determines the purpose and means of data processing, performs the processing operations, and is responsible for this processing.

The controller is any natural or legal person or any organisation without legal personality that determines the purpose of the processing of data, makes decisions on data processing (including those as to the means of the processing) and implements such decisions or has them implemented by the technical data processor he has commissioned.
In the course of employment a distinction could be made between the data controller and other persons performing data controlling. The data controller is the company or person who employs the data subject. The employer within the data controller or the company, i.e. the manager is entitled to get acquainted with the personal data of an employee.

Processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Processor

The controller does not have to perform all the activities related to the processing of personal data himself. He may authorise another subject to carry out the processing, in whole or in part. The processor does not become the controller of data the processing of which has been entrusted to him. The fact that the entity entrusted with data processing does not become their controller carries specific consequences. The obligations imposed by the legislation on the controller, e.g. the duty to register, do not apply to this entity. It is nevertheless obliged to safeguard the data.

The Act requires that the contract on entrusting another entity with the processing of data shall be drawn up in writing and shall clearly specify the scope and purpose of data processing. As regards the compliance with the requirements on safeguarding data, the processor shall bear the same responsibility as the controller. Moreover, the entity entrusted with data processing shall be responsible to the controller in respect of activities, which are inconsistent with the contract concluded with the controller.
The Inspector General for Personal Data Protection shall be responsible for oversight of compliance with the provisions on personal data protection with respect to data processing done by the entity entrusted with processing. The oversight shall be exercised pursuant to rules laid down in Article 14–19 of the Act on the Protection of Personal Data (Article 31 para. 5 of the above-mentioned Act).

In the case the authorization is not legally grounded, the controller and processor shall conclude an agreement on the processing of personal data pursuant Article 6 of the Data Protection Act. The agreement has to be in writing. In particular, the agreement shall explicitly stipulate the scope, purpose, and period of validity as well as provide for the processor's guarantees regarding the technical and organizational aspects of data security.
If the processor finds out that the controller violates the obligations laid down in the law, it is its duty to notify such breaches without delay and to discontinue the processing in question. Failing to do that, the processor and controller can be jointly and severally held liable for any damage such data subject has suffered.

If the processing is subject to notification obligation, the duty to submit the notification to the Data Protection Authority rests with the controller.

There are no specific national variations.

Third party

> Third party shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

The notion of third party is of paramount importance for the activity of entrepreneurs, since disclosure of personal data to third parties entails numerous obligations, such as the existence of a valid legal basis or the obligation to protect the data against third party access for which no such legal basis exists. It should be noted that it is not the controller himself, neither the persons authorized by him to process the data or the processor that shall be treated as a third party. Not all national legislations regulate this. However the notion of the controller, the person authorized to process the data or the processor provide an indirect definition of the third party.

There are no specific national variations.

There are no specific national variations.

Employment creates a legal relation between the employer and the employee. Except for the employer acting as a data controller and other persons authorised to control data in course of employment, all other participants can be treated as third parties under the Data Protection Act and the Labour Code. Transferring data to third parties may be slower, because there is no legal authorization to do so and all employees concerned have to consent to such operation.

Recipient

> Recipient shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

In order to ensure that data subjects have the possibility to control their personal data, the entrepreneur is required to inform them about known recipients of the data that he is processing.

Data recipient shall mean any person to whom the data are disclosed, with the exception of:
a) the data subject,
b) a person authorised to carry out data processing,
c) a representative of the controller established in a third country, who is using the means,
d) a subject referred to in Article 31,
e) state authorities or territorial self-government authorities to whom the data are disclosed in connection with conducted proceedings.

Recipient is any subject to whom personal data are disclosed. Recipient is not a subject that processes personal data for the purposes of inspection, supervision, and regulation related to the exercise of public authority.

The Data Protection Act refers to this concept, but does not define it. The recipient is usually the data controller. It is not a new status. The status of the data controller shall be distinguished here from the data recipient.

The data subject's consent

The data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

It means any freely given, specific and informed indication of the wish of the data subject by which he expresses his unmistakable agreement to the processing, either wholly or partially, of his personal data. Such consent may be withdrawn. The consent to the use of sensitive data needs to be given in writing.

The consent cannot be alleged on the basis of a declaration of will of the other consent. The declaration of will has to be singled out.

Consent of a data subject is defined as any free and informed manifestation of the data subject's will. Such consent includes the data subject's acceptance of the processing of his personal data. The Data Protection Act, although it does not provide for a written form, requires that the consent must be verifiable for the duration of data processing.

It has to be decided on a case-by-case basis whether the Labour Code or the consent serves as authorization for the data processing. There are only a few sector specific legal regulations. The consent of the data subject seems to be a better legal safeguard in view of the fact that in many cases, legal authorization is questionable.

3. The legitimacy and compliance of the business activity

Basic obligations concerning data processing

A data controller must be able to demonstrate that the relevant legal prerequisites for data processing are met. The controller also, has to fulfil the information obligation and ensure the quality of the processed data. Furthermore, he is obliged to respect the data subjects' rights, properly safeguard the data and notify the data filing systems he keeps to the national data protection authority in order to register them.

Legitimacy of personal data processing

Each data processing operation needs to have a valid legal grounds. By "legal grounds" we mean an authorization to process personal data within a specified scope.
The data subject's consent or an obligation to process personal data arising from law are examples of such grounds.
As a rule, the processing of sensitive data it is prohibited. However, in some instances the controller is allowed to use such data, if he can prove that he is dealing with an exceptional case so defined under data protection national laws.

The processing of data is permitted only if:

- the data subject has given his/her consent, unless the processing involves erasing personal data,
- the processing is necessary for the purposes of exercising the rights and duties arising from a legislative provision,
- the processing is necessary in order to perform a contract to which the data subject is a party or to take measures, at the request of the data subject, before signing a contract,
- the processing is necessary in order to perform tasks provided for by law and carried out in the public interest,
- the processing is necessary for the purposes of legitimate interests pursued by the controllers or data recipients, provided it does not violate the rights and freedoms of the data subject. Here, legitimate interests are considered to be: direct marketing of one's own products or services provided by the controller, or assertion of claims resulting from economic activity.

These prerequisites are separable. In order to consider the use of data to be legitimate, it is sufficient to meet one of them, and not all of them jointly. Therefore, if rights and duties resulting from a legal provision cannot be exercised without the use of data, then no additional consent for their use is required. Neither is it necessary to justify that the processing is carried out in the public interest or for the purpose of legitimate interests pursued by the controllers. Consent for the use of data to exercise a legal norm is confusing, because it suggests that it may be withdrawn if the transfer of data is required for the purposes of data collection.
The use of sensitive data is, as a rule, prohibited under Article 27 (1) of the Act. However, such data can be used by a controller, provided he proves that it is one of those exceptional situations referred to in Article 27 (2) of the Act.

The processing of sensitive data inter alia is permitted in the event that the data subject has given his/her written consent or specific provisions of other enacted laws allow it, providing for adequate safeguards. The processing of sensitive data is also allowed when it is necessary to protect the vital interests of the data subject or of another person; when the data subject is physically or legally incapable of giving his/her consent until a guardian or a curator is appointed; when it is necessary to carry out the duties of a controller relating to the employment of his/her employees and other persons, and the scope of data is provided by the law; when it is required for the purposes of preventive medicine, the provision of care or treatment, when the data are processed by a health professional engaged in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards.

The main legal grounds for making data processing legitimate is the data subject's consent. The Act 101 provides for a set of requirements that must be met when seeking such consent. It is important to bear this in mind, because consent is sometimes misused as a tool violating other instruments of personal data protection.
The consent must be explicit. Data subject gives his/her consent to a controller. Processing of data could not take place without this legal act being accomplished, and the consent itself would lose any sense. Consequently, the consent may be interpreted as a proposal to enter into a certain contract, or it may be incorporated into a more complex agreement. Consent may in no way be understood as an isolated one-sided act.
Without such consent, the controller may process data:

- if he is carrying out processing which is essential to comply with legal obligation of the controller;
- if the processing is essential in order to perform a contract to which the data subject is a contracting party or enter into negotiations aimed at concluding or amending a contract at the request of the data subject;
- if it is essential for the protection of vitally important interests of a data subject. In this case, the consent of the data subject must be obtained without undue delay. If the consent is not granted, the controller must terminate the processing and erase the data;
- in relation to personal data that were lawfully published in accordance with special legislation. However, this shall not prejudice the right to the protection of private and personal life of the data subject;
- if it is essential for the protection of rights and legitimate interests of the controller, recipient or other person concerned. However, such personal data processing may not contradict the right of the data subject to protection of his private and personal life;
- if he provides personal data on a public figure, a public administration official or employee disclosing information about their public or administrative activity, their function or work position;
- if the processing is done exclusively for archival purposes, pursuant to a special statutory law.

The legal grounds for processing sensitive data are laid down in Article 9 of the Act 101.

According to the main rule of the Hungarian data protection law, personal data may be processed only if an act passed by parliament so permits or the data subject consents to the processing. In the case of sensitive data, the consent to their processing must be expressed in writing.

According to point 6 of Article 2. of the DP&FOI Act, consent means any freely given, specific and informed indication of the wish of the data subject by which he signifies his unmistakable agreement to the processing, either wholly or partially, of personal data relating to him.
The Act does not specify the scope of personal data that may be processed by the employer. According to Article 77 of the Act XXII of 1992 on the Labour Code *„(1) An employee shall only be requested to make a statement, fill out a data sheet, or take an aptitude test if it does not violate his personal rights and which essentially provides information considered substantive for the purposes of entering into an employment relationship."* An employer is authorized by law to process data by an act particularly specifying the scope of data, and may control data only in relation to such data (i.e. data related to social security, taxation, obligation to pay related contributions, etc.).

Remember:

- Always make sure before starting data processing that you meet at least one of the prerequisites for legitimacy specified in the relevant data protection act of the country concerned. Different legitimacy prerequisites may be applicable to similar data processing operations depending on the country.
- If consent is necessary, the controller needs to formulate the consent clauses explicitly and separate them from other declarations of will made by the data subjects.
- The collection of sensitive data is, as a rule, prohibited. However, if such data need to be collected for the purposes of running a business, it can be done provided that either the data subject expresses his/her written consent, or another legitimacy prerequisite is met.
- The consent has to be freely given, be specific and informed.

Data quality

The following principles ensure data quality:

1. The finality principle

   This principle, called also a **purpose limitation principle**, means that data must be collected for specified, legitimate purposes and not further processed where the further processing is incompatible with these purposes. This means that:
   - the party collecting data can neither omit nor hide this purpose,
   - the purpose of data processing cannot be stated vaguely,
   - the purpose shall be communicated to the interested person before personal data is collected,
   - it is prohibited to make the conclusion of a contract conditional on giving consent to the processing of data for completely different purposes (e.g. the marketing of products and services of third parties).

   The processing of data for purposes other than the one for which they have been collected is, however, allowed if it does not violate the rights and freedoms of the data subject and is conducted:
   - for scientific, historical or statistical purposes, and also for didactic purpose in Poland,
   - in compliance with the legitimacy prerequisites.

2. The accuracy principle

   A controller is obliged to ensure that the data are accurate, complete and up to date. To this end, in the course of data processing, the controller shall:
   - each time evaluate the credibility of the source of data,

– develop a mode of data accuracy verification (depending on whether the data are "regular" or sensitive) and establish a code of conduct in the event that data are found to be inaccurate,
– inform other controllers to whom he has disclosed the data about any update or rectification thereof.

Collection of data from sources of unknown origin, which do not guarantee their accuracy, shall be considered a violation of this principle. The processing of inaccurate, incomplete or not up-to-date data often cannot be conducted due to technical reasons (e.g. construction of IT applications used for personal data processing).

3. The proportionality/adequacy principle

In accordance with the adequacy principle, data must be relevant and not excessive in relation to the purpose for which they are processed. The controller shall only process data the type and content of which are necessary for the purposes of data collection. Relevance (adequacy) of data shall be assessed at the time of their collection, at the latest. Thus, the controller is obligated to verify this. The scope of personal data adequate for the purpose of the processing shall be assessed each time by considering a specific legal relationship, in connection with which the controller is processing personal data. As regards contracts, their character and importance need to be taken into account. Sometimes, the legislator expressly points to the scope of data adequate for the purposes of processing in the relevant legal provisions.

4. The time limitation principle

The controller is required by law to store data in a form which permits the identification of data subjects as long as it is necessary to fulfil the purpose for which they are processed. After such purpose is achieved (e.g. the performance of a contract, the expiry of the data storage period indicated in legal provisions) data shall be erased, anonymised or transferred to the entity authorised by law to receive such from the controller (e.g. State archives).

Remember:

- Processing starts when data is collected. The collection of data is a processing operation.
- You should only collect data closely related to the purpose of your economic activity.
- You cannot collect data "just in case", to be used in the future. No stockpiling of data is allowed.
- It is prohibited to make the conclusion of a contract conditional on giving consent to the processing of data for other purposes (e.g. marketing of products and services of third parties).
- You cannot use personal data collected from sources of unknown or unreliable origin, which do not guarantee accuracy. You always need to make sure that the collected data are accurate, complete and whenever possible, up to date. Therefore, you have to develop a mode of data accuracy verification and establish a code of conduct for situations when data have been found to be inaccurate.
- You should monitor, on a continuous basis, the content of your personal data filing systems keeping in mind the need to erase superfluous data.
- You cannot store data longer than it is necessary for achieving the purpose for which they have been collected.
- After achieving the purpose of data processing (e.g. after the performance of a contract), the collected data shall be erased, anonymised, or transferred to the entity legally authorised to receive them from the controller.

The controller's obligation to inform the data subject and the data subject's access to data

Prior to data collection, the controller needs to provide the data subject with specific information, the scope of which depends on whether data are collected directly from such data subject or from other sources.

Under the provisions of Directive 95/46/EC, if data is collected from a data subject, the controller shall provide the data subject from whom his data are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as:
  – the recipients or categories of recipients of the data,
  – whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  – the existence of the right of access to and the right to rectify the data concerning him;

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

In the case of data collected from sources other than the data subject, the controller must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing;
(c) any further information such as:
  – the categories of data concerned,
  – the recipients or categories of recipients,
  – the existence of the right of access to and the right to rectify the data concerning him;

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

The information obligation shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases, Member States shall provide appropriate safeguards.

In such case, informing the data subject about the principles of data use shall be the controller's obligation, regardless of the fact whether the data subject requests such information or not. At each subsequent stage of data processing, information shall be given when the data subject requests it.

From the beginning of data processing, every data subject has the right of access to data without constraint at reasonable intervals and without excessive delay or expense, for:

– confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
– communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;
– knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions.

Moreover, the data subject may request, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions on personal data protection, in particular because of the incomplete or inaccurate nature of the data.
It needs to be stressed that the scope of the information given by the controller and the mode of disclosure of information at the data subject's request may vary in different countries.

The information obligation is regulated in Articles 24 and 25 of the Act on the Protection of Personal Data.
If the data are collected from the data subject, the controller must provide the information in the scope indicated in Directive 95/46/EC at the time of their collection. This obligation shall not apply if: any provision of other law allows for personal data processing without a disclosure of the real purpose for which the data are collected or, just like in Directive 95/46/EC, the data subject already has the information which has to be provided under Article. 24.1 of the Act.
In the event that the data have not been obtained from the data subject, the controller has to fulfil the information obligation specified in Article 25.1 of the Act, and thus, save for the information indicated in Directive 95/46/EC, he has to inform the data subject of: the source of data, the right of access to his/her data and to rectify them, of the rights arising under Article 32.1(7) and (8) of the Act on Personal Data Protection, i.e. of the right to demand erasure of data due to the data subject's particular situation, or to object to the processing of his/her personal data for marketing purposes and to their transfer to other controllers.
It is very important that the information obligation be fulfilled immediately after the recording of the collected data, that is after recording the data in a way enabling their further processing.
Exemptions from this obligation are listed in Article 25.2 of the Act, pursuant to which it is not necessary to provide information where:

– the provision of other laws provides or allows for personal data collection without the need to notify the data subject,
– the data are necessary for scientific, didactic, historical, statistic or public opinion research,
– the processing of such data does not violate the rights or freedoms of the data subject, and the fulfilment of the terms and conditions laid down in Article 25.1 would involve disproportionate efforts or endanger the success of the research,
– the data are processed by public body or a body carrying out public tasks on the basis of legal provisions,
– the data subject already has the information to be provided.

The right of access has to be exercised within 30 days from the date of submission of the data subject's request, in the scope specified in Article 321 subpars. 1-5a. At the request of the data subject, the information is provided in writing. If the right of access is exercised less than every 6 months, then it is free of charge.
The information shall not be provided, if it would:

1. result in the disclosure of information containing classified content,
2. pose a threat to national defence or security of the state, human life and health, or security and public order,
3. pose a threat to fundamental economic or financial interests of the state,
4. result in a substantial breach of personal interests of the data subjects or other persons.

1. In complying with the obligation pursuant Article 11(1) of the Act 101 (conforming with Article 10 of Directive 95/46/EC) the fact that the personal data in question are already known can be taken as an exonerating circumstance. The information obligation can therefore be exercised through, for example, a clause providing for consent with data processing. Other exonerating grounds pursuant to Articles 10 and 11 of the said Directive are laid down in the Article 11(3) of the Act 101. In contrast, Article 11(4) imposes the explicit obligation to inform about processing pursuant Article 5(2)(e) and Article 9(h) (processing of personal data for the purposes of the protection of rights in accordance with the Article 7(f) and Article 8(2)(e) of the Directive 95/46/EC).
2. Controllers have the right, in connection with access to personal data pursuant Article 12(3) of the Act 101, *to charge an appropriate fee for providing information* to the data subject. The fee must not exceed the costs necessary to provide the information. The information obligation can be fulfilled by the processor on behalf of the controller.

According to Article 6 of the DP&FOI Act, prior to the collection of data, the data subject has to be informed whether it is voluntary or compulsory to supply the data. In the case of compulsory supply the rule of law ordering data processing shall also be indicated. The data subject has to be given unequivocal and detailed information on all the facts relating to the processing of his data, in particular on the purposes and legal basis of the data processing, on the person authorised to carry out the data processing and the technical data processing, the duration of data processing, as well as on who is authorised to have access to the data. Information shall also be given on the rights and remedies of data subjects in connection with the data processing. The information on data processing is considered to have been given where a rule of law orders the collection of data from an existing data file by transfer or combination. If it is impossible to inform each data subject, or if it would entail disproportionate expenses, particularly in the case of processing data for statistical or scientific (including historical research) purposes, information may be given by making public, in a way that it will be accessible to all, the fact of data collection, the data subjects concerned, the purpose of the data collection, the duration of the data processing, and the accessibility of the data.

Article 12 of the DP&FOI Act provides that the data controller has to inform the data subject, upon his request, of the data processed by the data controller or technically processed by the technical data processor, of the purpose of the data processing, of its legal basis and duration, of the name, address (seat) and activity of the technical data processor in connection with the data processing, as well as of those who received or will receive data and for what purpose. The duration of records on transfer and, on the basis thereof the obligation to give information, may be limited by rules of law on data processing. The limitation may not be shorter than five years with regard to personal data, or twenty years with regard to special data. The data controller gives the information in writing and in an easy to understand way, within the shortest possible time, but not later than within 30 days, of the lodging of the request. The aforementioned information is free of charge, unless in any given calendar year, the person requesting information has already filed a request with the data controller for the same field. In other cases expenses may be charged. Such expenses may be refunded where the data have been unlawfully processed or where the request for information has resulted in rectification.

The rights of the data subject may be restricted by an Act in the interest of the external and internal security of the State, such as national defence, national security, crime prevention or criminal investigation, for the economic or financial interests of the State or the local government, for important economic or financial interests of the European Union, for the prevention or exposure (including in all cases, supervision and control) of professional disciplinary or ethical offences or of breaches of labour law or work safety obligations, as well as for the protection of the rights of data subjects or of other people (Article 16 of DP&FOI Act).

Remember:

- You should directly inform the data subject that you are going to collect his/her data before starting the collection of his/her personal data. The information must be provided individually and cannot be made in another form, e.g. by announcement or note posted, for example, in a regulation, if the person concerned has no possibility of directly acquainting himself with the content of such documentation.
- There is no specific form of providing the data subject with information about the start of the data collection (it might be in person, in writing, by phone etc.), although it is recommended to use the formal way (e.g. written form). It should be remembered that in the event of a potential dispute relating to the fulfilment of the information obligation, the controller shall be obliged to provide evidence proving that this obligation has been fulfilled.
- You should always make the information you have gathered accessible to the data subject.
- The data subject has the right to access the information, to correct them or to erase the data or to demand a stop to further processing of the data.
- If you did not obtain the information directly from the data subject (e.g. you bought the data filing system from other company), you should immediately inform the data subject about processing the data and the source of information. You cannot undertake any marketing activities without informing the persons whose data you have indirectly obtained and without giving them the possibility to object to the processing of their data for marketing purposes.

Data security

One of the basic obligations of the controller is to ensure data security, i.e. to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The applied measures must be commensurate with the risk and category of data and reflect the state of the art in this field. Ensuring data security is a continuous process, which involves risk analysis and should also consider variable circumstances affecting the level and nature of existing risks.

The obligation to secure data is imposed on every controller (regardless of his size) and entity commissioned to process the data.

Safeguarding data entails not only adopting organisational measures, such as preparing special documentation describing the processing of data and their protection, or appointing an administrator of information security, but also adopting strict technical measures.

Implementation of security measures may be connected with the need to apply recognised security standards or to apply directly provisions on personal data protection, which can sometimes contain detailed requirements in this regard.

Security measures should depend on the environment in which the data are processed. As regards IT networks, the security of personal data may be regarded as being similar to information security, which means ensuring confidentiality, integrity, availability, accountability, authenticity, non-repudiation and reliability. These terms have the following meanings:

Confidentiality – ensuring that the information is not made available or disclosed to unauthorised persons, entities or processes,

Integrity – ensuring that the data have not been changed or destroyed in unauthorised way,

Availability – ensuring to be available and possible to use at request, within specific time, by authorised entity,

Accountability – ensuring that the entity's activities may be assigned unequivocally only to this entity,

Authenticity – ensuring that the entity's or resource's identity is the same as the one declared (authenticity applies to users, processes, systems and information),

Non-repudiation – no possibility to deny one's involvement, in whole or in part, in data exchange by one of the entities involved in this exchange,

Reliability – ensuring coherence and intended behaviours and results.

It needs to be stressed that ensuring and then demonstrating specific characteristics often requires applying specific measures and meeting many conditions at the same time.

The controller is obliged to, *inter alia*:

- appoint an administrator of information security who will supervise the processing (it is recommended that this person be knowledgeable about personal data protection essential for an effective performance of this function), unless the controller performs this function himself;
- keep the documentation describing the data processing method and undertaken technical and organisational measures, this documentation should include security policy and IT system management instruction;
- ensure oversight of data, when and who entered the data into the filing system and to whom they are transferred. The exercise of such supervision is specified by the controller, taking into consideration the undertaken organizational and technical measures;
- grant authorisations to persons having access to personal data.

The obligation to authorise persons arises from Article 37 of the Act. Considering the purposes of providing evidence and the need to keep a record of authorisations, the authorisation shall be drawn up in written form and include the name (surname), name and surname of the person granting the authorisation to process personal data, the date of granting it and the expiry date. The scope of data to which a person has access and the name of the data filing system have to be specified as well. The record of authorised persons has to include the following information: name and surname of the authorised person, the date it was granted, the expiry date and the scope of authorisation to process data, as well as the identifier, if the data are processed in an IT system. The persons authorised to access the personal data must keep them secret.

Specific conditions of safeguarding personal data are set forth in Regulation of 29 April 2004 of the Minister of Interior and Administration as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for personal data processing. The Regulation also provides for security measures to be applied to data protection. The choice of measures depends on the data security level in the IT system adopted for a given data filing system.

Article 13 of the Act 101, going beyond the framework of Directive 95/46/EC, imposes on the controller and the processors the obligation to respect certain risks and to adopt further and more specific measures. It applies in particular to these obligations:

1. To develop and document technical and organizational measures ensuring protection of personal data.
2. To meet, in case of automatic processing of data, the following requirements:
   - to ensure that the systems for automatic processing of personal data are used only by authorized persons;
   - to ensure that natural persons authorized to use systems of automatic processing of personal data have access only to the personal data corresponding to their authorization, on the basis of specific user authorizations issued exclusively to such persons;
   - to make electronic records that enable identification and verification of when, by whom and for what reasons the personal data were recorded or otherwise processed, and
   - to prevent any unauthorized access to data carriers.

Provisions of Articles 17(2) and 17(3) of the said Directive concerning relations between controllers and processors are taken into account in Article 6 of the Act 101 which provides for the possibility of them entering into a contract. Responsibilities of the processor are regulated by a number of provisions of the Act 101, namely by Articles 7 and 8. Article 16 of Directive 95/46/EC is transposed by the Articles 14 and 15 of the Act 101.

Article 10 of the DP&FOI Act provides for the rules of data security specifying the requirements of processing. Ensuring data security and taking all technical and organisational measures and elaborating the rules of procedure necessary to enforce compliance with the Act and other rules pertaining to data protection and confidentiality fall within the scope of the data controller's and/or processor's responsibilities. Data has to be protected, in particular, against unauthorised access, alteration, transfer, making public, deletion or destruction, as well as against accidental destruction or damage. If personal data are transferred via a network or other information technology equipment, the data controller, technical data processor and the operator of the telecommunications or information technology equipment should take special protective measures to ensure that personal data is technically protected.

Article 31/A of the DP&FOI Act specifies cases when the appointment of a data protection officer or the adaptation of data protection and data security rules are mandatory. This article provides that an internal data protection officer holding a higher education degree in law, public administration or information technology, or a qualification equivalent thereto, shall be appointed or commissioned within the organisation of the data controller or of the technical data processor and he shall report directly to the head of the following bodies:

- data controllers or technical data processors performing the processing or technical processing of data files of national authorities, or of national labour or criminal data files;
- financial organisations; and
- providers of telecommunications and public utility services.

The internal data protection officer can be an employee of the data controller; or be assigned to this function.

The internal data protection officer shall:

a) contribute to or assist in taking decisions related to data processing and to the enforcement of the rights of data subjects;
b) monitor compliance with this Act and other rules of law on data processing, as well as with the provisions of internal data protection and data security rules and with data security requirements;
c) investigate reports submitted to him, and call on the data controller or technical data processor to discontinue any unlawful data processing observed by him;
d) draw up the internal data protection and data security rules;
e) maintain the internal data protection register; and
f) ensure the training of the staff in data protection.

Data controllers who have an obligation to appoint an internal data protection officer shall be required to adopt data protection and data security rules. Data protection rules are internal and binding rules within the organisation that describe the details of the data processing and foster the implementation of data protection laws and the exercise of the data subjects' rights. The DP&FOI Act does not specify the content of data protection rules in this respect. It would also be difficult to create unified data protection rules, because of the variability of the data processing activities. However, the main questions to be ruled can be summarized thus:

– to adapt the rules of the DP&FOI Act to individual needs;
– to endorse the data protection within the organization;
– to define access rights;
– to define the control mechanism;
– to clearly spell out responsibility;
– to specify the particular data procession sets.

It means that the data protection rules are internal, binding instructions ordered by the head of the organization.

This concept has got high significance in the practice of commissioners. It has been applied when the legal authorization of the data processing was doubted. For instance, the information given to the data subject has to be detailed, and when the information is unclear, or inaccurate, the data subject may misunderstand it. Thus the data controller is found in breach of the requirement that obtaining and processing of data should be fair and lawful, which is included in the principle of data security.

Remember:

- In safeguarding personal data, the existing risk to and the nature of the data being processed should be taken into account.
- Only persons duly authorized by the controller can have access to data. Special requirements specifying the form of authorisation may exist in particular countries.
- The controller should develop special internal documentation, aimed at describing data processing procedures, indicating activities to be performed as well as specifying the principles and rules of conduct, which shall be applied in order to adequately safeguard personal data. The documentation should translate into the everyday activity of the controller.
- The controller should also specify the control method in order to supervise the processing of the data, especially what data, when and by whom have been entered into the filing system and to whom they are transferred.
- The controller and all the persons authorised to process the data must keep them and their security arrangements secret.

Notification obligation

The data controller shall be obligated to notify a personal data filing system to be registered by the Data Protection Authority of the country, where the company is established. This obligation exists in Poland, Czech and Hungary, although its methods may differ depending on the country. Certain exceptions to the general principle of notification exist and are enumerated in the national data protection legislation.
Before notifying a data filing system for the purposes of registration, each data controller shall check whether the data filing system that he maintains is exempt from the notification obligation pursuant to these provisions.
Please bear in mind that registration is not the sole obligation imposed on the controller.

Pursuant to Article 40 of the Act, the controller is obligated to notify a personal data filing system for the purposes of registration by the Inspector General for Personal Data Protection. Exceptions to this rule are enumerated in Article 43.1 of the Act. Before notifying a filing system, each controller should check whether the data filing system that he maintains is exempt from the notification obligation pursuant to these provisions.

The notification method.
A data filing system shall be notified for the purposes of registration on a form whose specimen is published in the implementing ordinance to the Act.
Any change of information that has been earlier notified for the purposes of registration is subject to notification (within 30 days following the date of the change). So, if the terms and conditions of keeping the filing systems change, such change has to be notified to the Inspector General for Personal Data Protection. Information about discontinuation of personal data processing has to be notified as well.
A party may be summoned to present other documents, which may be of importance (an excerpt from the National Court Register, a security policy document, an IT system management instruction) in connection with a case initiated under administrative proceedings applied by the Inspector General for Personal Data Protection to register a filing system.
The notification of a data filing system for the purposes of registration and its updates can be sent by post, submitted in person or by using the electronic platform for communication with the Inspector General for Personal Data Protection, the e-giodo platform, available at www.giodo.gov.pl.
The e-giodo system allows online notification of data filing systems and their updates for the purposes of registration. In such case, the notification form is filled in using an application installed at www.giodo.gov.pl. It provides helpful tips and information to the applicant on how to correctly fill in the form. After filling it in, the application can be sent electronically by entities that have electronic signature. The form filled online can also be printed out and sent by traditional method.

Certificate of data filing system registration.
The controller of ”regular” registered data may commence their processing once the filing system has been notified to the Inspector General. The certificate of registration of a data filing system is then issued at the request of a controller.
The controller may commence the collection of sensitive data only after registration of the data filing system. The Inspector General for Personal Data Protection is obligated to issue a certificate promptly upon registration of data filing system.

Examples of exemption from the obligation to notify a data filing system for the purposes of registration:

– Registration of employees and job applicants' data
  The exemption from the registration obligation under Article 43.1(4) of the Act applies to filing systems containing data processed in connection with employment with the controller (i.e. filing systems with data of current and previous employees, as well as job applicants) and the provision of services to the controller pursuant to civil law contracts (e.g. a mandate contract or a contract for the provision of specific work). Such data files do not have to be notified.
– Registration of a data filing system for the purposes of maintaining day-to-day relations
  The obligation to register a data filing system shall not apply, if the data contained therein are publicly available (Article 43.1(9)) or are processed in connection with minor current day-to-day affairs (Article 43.1(11)).
  The processing of data for the purposes of maintaining contact with a person representing an entity or in the scope necessary to achieve this purpose is aimed at improving the data controller's activity. Thus the data contained in such filing system may be treated as data processed with regard to minor day-to-day affairs.

Notification is free of charge.

Registered data filing systems are disclosed in the national register of personal data filing systems, available online.

Controllers are obliged to notify the OPDP of the intended or already running processing of personal data. The notification is done through a formalised procedure (either in writing or electronically) pursuant Article 16(2) of the Act 101.

Not every processing operation is subject to the notification obligation. Exemptions are laid down in Article 18 of the Act 101. In particular situations set out in this Article, controllers are required to fulfil a special information obligation, i.e. to ensure that required data be made available by remote access or in another appropriate form.

The Act 101 lays down the rules of registration. It is not regulated by the administrative procedure law.

Once the registration form is submitted to OPDP, its content is checked for completeness and, if necessary, the controller is requested to provide additional information within a certain time. If the controller fails to do so, the submission is considered as not having been made.

If any information contained in the submitted notification raises concerns about potential breach of law committed during the notified processing operation, the OPDP is authorised to initiate proceedings pursuant to the Administrative Code. The controlling staff can naturally come to the conclusion that there is no risk of any violation of law and the proceedings may then be discontinued. If the opposite is the case, the OPDP orders the said processing operation to be stopped. These proceedings are very similar to the procedure of prior checking laid down in the Act 101 (in the meaning of Article 20 of Directive 95/46/EC).

If the purpose of processing no longer exists, the OPDP may decide (on its own initiative or upon the controller's request) to revoke the registration. The OPDP may also cancel the registration in the event of a breach of law by the controller. The controller is obligated – if it plans to discontinue its operations – to inform the OPDP about how it intends to treat the previously processed data that has been notified and registered with the OPDP.

Notification and subsequent registration are free of charge.

The OPDP uses notifications to maintain a register of processing operations. This register is accessible to the public on the OPDP's website. Revoked registrations are published regularly in the OPDP's Official Journal. Only information concerning processing methods and data security measures are not publicly accessible.

Article 28 of the DP&FOI Act provides that prior to commencing his activity, the data controller who processes personal data shall notify the Data Protection Commissioner, for the purposes of registration, of the following: the purpose of data processing; the data categories, and the legal basis of their processing; the scope of data subjects; the source of data; the categories and recipients of transferred data, and the legal basis of the transfer; the time limits for the deletion of certain types of data; the name and address (seat) of the data controller and of the technical data processor, the actual place of data processing or technical data processing, as well as any activity of the technical data processor related to the processing of data. The Data Protection Commissioner enters the data processing in a public register.
This registry is not an authority register, it does not commence right to the data processing. Failure to notify or improper notification can constitute grounds for the Data Protection Commissioner to start an investigation.
Data controllers shall notify in the data processing except data processing categories which are named in Article 30 of DP&FOI Act. The data of persons having an employment shall not be notified. This exception also applies also to the relationships similar to the employment relationship and also in other legal relationships. However, prior to commencing their activity, enterprises have to notify other data processing categories not listed as an exception in the DP&FOI Act, like the data processing of any direct marketing activity.
The notification is free of charge and may be filled in and submitted electronically, with its duly signed hard copy sent to the Data Protection Commissioner since a notification is treated as a representation.

Remember:

- In Poland, Czech and Hungary, the notification/registration obligation is one of the basic obligations of data controllers.
- In particular EU Member States, there may be differences in notification of data filing systems for the purposes of registration. Therefore, when undertaking economic activity in another EU Member State you should always get acquainted with the relevant legal provisions on the notification obligation.
- Particular Member States may apply exemptions from registration of data filing systems. The employee data filing system may serve as an example. The list of exemptions may differ from country to country.
- Failure to notify a data filing system for the purposes of registration, as required by the applicable law, may result in a liability, civil or administrative, for the violation of personal data protection laws.
- A change of notifiable information and the discontinuation of a filing system require notification within specified time limits.
- It is recommended to notify online. Therefore, you should visit the website of a particular personal data protection authority to find out about such option.
- Both notification and update of the filing system must be done in the official language of a given country.

Data transfers to third countries

Transferring personal data among entrepreneurs in Poland, the Czech Republic and Hungary, as well as transferring data to entities in other EEA Member States (EU Member States and Iceland, Liechtenstein and Norway) is treated like any other data processing in each of the partner countries and does not give rise to any additional obligations.

There are additional requirements relating to the transfer of data to third countries (which are not members of the EEA). Apart from additional requirements, all the other obligations arising from legal provisions on personal data protection have to be met.

As a rule, data may be transferred only to recipients in third countries, which ensure an adequate level of personal data protection. Very often these are countries with regard to which the European Commission has issued special decisions acknowledging that they offer adequate level of data protection.

Individual data protection acts provide detailed principles of transferring data to third countries. In particular for countries that do not ensure an adequate level of protection; such provisions include specific legal grounds for data transfer and may require special authorization (permission) to be obtained from the relevant data protection authority.

If the recipient country does not ensure an adequate level of protection, the data subject must be informed thereof, i.e. of the risk of possible violations of the data processing rules. Very often, the controller has to guarantee that the data recipient ensures an adequate level of protection of personal data and of the data subject's rights.

Adequate protection can be guaranteed in a number of ways by controllers or by processors operating in third countries:

a) By applying a set of standardized provisions adopted by the European Commission and called "Standard Contractual Clauses".
   They provide a legal basis for transfers from EU Member States to third countries. There are two kinds of such clauses – one group provides for data transfers to data controllers established in a third country, while the other regulates transfers to data processors
   In view of the complexity of the issue, you are recommended to consult your national data protection authority.

b) By applying ad hoc contractual clauses.
   In addition to the European Commission's Standard Contractual Clauses, data controllers and data processors in third countries and organisations transferring data may also determine the conditions of data transfer and conclude an agreement thereon. The agreement must ensure adequate level of personal data protection during data processing by the controller or by the processor.

c) By applying Binding Corporate Rules (BCRs).
   Binding Corporate Rules are typically developed and applied by multinational companies in order to regulate data flows between different units of the company located in different countries (also outside the EU). BCRs allow international enterprises to regulate data exchange between their many units with a single internal data protection document, so that units affected by an exchange of data do not have to conclude agreements with other affected units.

The transfer of personal data to third countries that do not ensure an adequate level of personal data protection may take place only if:

– the data subject has given his/her written consent to the transfer of his/her data to third countries,
– it is provided for by a ratified international agreement or a legal regulation,
– the transfer is necessary for the performance of a contract between a data subject and a 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 controller and another subject,
– the transfer is necessary or required by reasons of public interest or for the establishment of legal claims,
– the transfer is necessary in order to protect the vital interests of the data subject,
– the transfer relates to data that are publicly available.

Under Polish law, if a country of destination does not ensure adequate data protection standards, the transfer of data may take place subject to a prior consent of the Inspector General, provided that the controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject (Article 48 of the Act). It should be emphasised that the transfer of personal data to a third country, which does not ensure an adequate protection level is possible only after an affirmative decision has been issued by the Inspector General. This means that the transfer of personal data is illegal before such decision is issued. When considering the request for consent, the Inspector General must assess whether the controller ensures an adequate level of privacy, rights and freedoms of the data subject. Each request is considered on a case by case basis, on the grounds of the facts of the case.

Prior to transferring data abroad, controllers have to seek permission from the OPDP. This permission (authorization) is not required if an international agreement or decision of an EU body provide for the free movement of data. Therefore, countries providing an adequate level of protection are those which have ratified the Council of Europe's Convention 108 and have enacted relevant legislation on personal data protection.

However, controllers established outside the EU that process data in the Czech Republic are obligated to nominate and authorize a processor having its seat in the Czech Republic.

Information about the method of seeking and obtaining approval to transfer data abroad is found on the ODPD's website at http://www.uoou.cz/ .

According to Paragraph (1) of Article 9 of Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (the Data Protection Act), personal data shall not be transferred to data controllers or data processors in third countries, unless the data subject has given his or her explicit consent or an Act of Parliament so provides, and an adequate level of protection of the personal data in the third country is ensured during the processing by the controller or the processing by the processor of the transferred data. Authorisation by the data protection authority is not required.

In practice, these rules are generally complied with in a way that the data subject employee's explicit consent must be obtained, since there is no Act of Parliament now in place that would provide for the transfer of data in employment relationships.
It is important to note that if the data subject has given his explicit consent to the transfer of his data, then the condition of an adequate level of data protection in the third country does not apply, and consequently it is not necessary, although naturally it is recommended to examine whether this condition has been fulfilled. According to the established data protection practice, if the destination of data transfer is a country which does not ensure an adequate level of protection, the data subject should be informed thereof, i.e. of the risk of possible infringements of the data processing rules. Only after being informed, can the data subject give his explicit consent, as required by law. If he lacks such information, he is not in a position to decide how his rights might be affected by the data processing.
The question often arises whether the consent of the data subject is needed also in the case of data transfer to EEA countries, because this is considered as data transfer within the territory of the Republic of Hungary. In view of the fact that, pursuant to Article 8, the consent of the data subject is necessary for data transfer (i.e. a data processing operation by the controller) even if it is carried out within the territory of Hungary, the consent of the data subject is likewise necessary for data transfer to EEA countries. If, however, the data are not transferred to an EEA country for data processing by the controller but merely for data processing by the processor, it suffices to inform the data subject thereof. In the latter case, the consent of the data subject is not necessary since it is also not necessary in Hungary either for data transfers with the purpose of data processing by the processor. If, however, the data are not transferred to an EEA country, but to another third country, the consent of the data subject must be obtained, because the above cited Paragraph (1) of Article 9 explicitly mentions transfer for the purpose of data processing by the processor.
As we have seen above, according to the Data Protection Act, ensuring an adequate level of data protection is not a precondition of the legality of data transfer, if the data subject gives his consent. Nevertheless, the person or organisation transferring the data and the addressee of the transfer (i.e. the data exporter and the data importer) may conclude an agreement in order to ensure an adequate level of protection, using either BCRs or the Standard Contractual Clause packages referred to in the Decisions of the European Commission. However, it is important to underline that the existence of such an agreement does not provide a legal basis for data transfer. It can merely ensure a level of protection. Thus, as it has been said , generally it is necessary to obtain the consent of the data subject.

Remember:

- The transfer of data to Poland, the Czech Republic or Hungary, or other countries, which are members of European Economic Area is treated like an in-country transfer and does not require any additional guarantees.
- The transfer of data to third countries imposes additional requirements and, as a rule, is possible, provided such country ensures an adequate level of personal data protection.
- Before intending to transfer data, you should carefully check the conditions to be met under the laws of particular countries, e.g. if an authorisation by the data protection authority is required.
- Meeting the requirements related to data transfer to third countries does not constitute a prerequisite of personal data processing legitimacy.

- Data may be transferred to third countries only for the purposes of processing operations, which are legally permitted in particular EU countries.
- If authorisation is required for data transfer, the appropriate request must be drawn up in the country's official language and it has to meet all the formal requirements provided for by national law.

4. Personal data as a subject of business activity

4.1 Processing of data in business life cycle

Setting up a business entails publication of different information on the entrepreneur and on the employees. Therefore, special attention should be paid to all activities related to collecting and further processing of personal data in each area of the company's activity and at every level of its internal hierarchy.

Company registration

While thinking of undertaking or expanding a business activity in another EU Member State, entrepreneurs should become familiar with specific legal provisions on registration of a business activity. When starting a business, entrepreneurs have to register their company in public registers, which include registers of entrepreneurs, of the statistical office, of the social insurance office, the tax office etc. The scope of information to be given depends on the form in which the business activity will be conducted. Entrepreneurs may be also obligated to use trade specific information which identifies them.

Entrepreneurs wishing to conduct one-man business or do business jointly with another entrepreneur under a contract of partnership shall make a proper notification on the official form to the competent municipal head, administrator or mayor who keeps a Register of Business Activity. Under Article 7a of the Act on Business Activity, data already entered in the register are not subject to the protection of personal data. This provision does not specify which data are subject to entry in the register of business activity. It only indicates the information which will be included in the application for entry in the register of business activity, i.e.: the name of an entrepreneur and his personal identification number (PESEL number), if any, the place of residence and address of the entrepreneur, and if he permanently conducts his business activity outside of his place of residence – also such place and the address of the main company, branch or another place, the subject matter of the conducted business activity based on the Polish Classification of Activity (PKD) and the date of commencement of the business activity. In the application for entry in the register of business activity it is important to include information on the entrepreneur closely connected with his business activity. Moreover, although the register is public, the materials on the basis of which the entry is made, including information not directly related to the conducted business activity, are not public.

Article 37.1 of the Freedom of Business Activity Act, which entered into force on 1 July 2011, is worth noting. This Article provides for the disclosure of data and information on entrepreneurs who are natural persons as specified in Article 25.1, except for their PESEL number and residence address, if it is the same as the place where business activity is conducted. The PESEL number does not identify an entrepreneur, but only a natural person. Thus, the legislator's intention was to disclose information relating exclusively to the business activity conducted by the entrepreneur in the register, not information on his privacy. The fact that personal data entered in the register is disclosed does not mean that they can be distributed by the registry office or processed by entities which obtained the data from the registry office. The Act on Personal Data Protection shall apply to such cases.

In connection with the setting up and running of a company, personal data of entrepreneurs are stored, in two public registers established by operation of the Commercial Code (Act No. 513/1991 Coll.) and the Trade Licensing Act (No. 455/1991 Coll.): the Commercial Register (Obchodní rejstřík) and the Trade Register (Živnostenský rejstřík).
In the Commercial Register keeps the following information: the name, surname, home address, birth number (or date of birth if birth number has not been allocated) of the entrepreneur who is the statutory body of a legal entity. The same data may be collected also on members of the legal entity's statutory body, or other entrepreneurs in cases specified in the Commercial Code. The Company Register is publicly accessible. The Trade Register is public as well, except for birth numbers and the list of fines imposed on entrepreneurs (traders) in connection with the conduct of their business activity.

Business is conducted mainly by organisations (companies) and entities which are not natural persons. Companies are set up and registered with the representation of natural persons, whose identification data shall be provided from a reliable source (i.e. an ID card). In the first stage of setting up a business activity, the most important is to present exact identification data of natural persons concerned.
Certain personal data of owners and representatives of companies are public both at stage of setting up and running of a business activity. Public access is a basic principle of the Hungarian company register (cégnyilvántartás). The names, domicile addresses and tax numbers of company representatives are publicly available data found in company registers.

Commencing business activity

Commencement of a business activity is connected with the need to fulfil various obligations resulting from the legal provisions on personal data protection, depending on the scope of data processing to be carried out within such activity and on the processing operation commencement date. Undoubtedly, while setting up a business, the entrepreneur should analyze for what purposes and in what scope personal data will be processed, as well as to ensure that the requirements specified in chapter two of the manual are met, in particular to ensure legitimacy, adequacy, the performance of the information obligation, data security, and if such obligation exists – notification of personal data filing systems for the purposes of registration.
From a practical point of view, at the start of a business, it is crucial to draw up documentation of personal data processing and to notify the kept data files for the purposes of registration before starting personal data processing of these files. If personal data collection is envisaged, proper forms with appropriate contents need to be developed.

Liquidation of the company/ closing of the business

In the event of a liquidation or bankruptcy of the entrepreneur, it is possible to process the information which identifies this entrepreneur or his representatives. The rules of conducting such proceedings are specified in separate provisions regulating bankruptcy proceedings and reorganization proceedings. In this context, it should be borne in mind that entrepreneurs can also be entered in various types of debtors' registers, as provided for under separate regulations. Liquidation of a company does not exempt the entrepreneur or persons conducting the proceedings from the obligations resulting from the provisions on personal data protection. In particular, one

has to remember about complying with the principle of finality and legitimacy of personal data processed by such entity.
After a business is closed, there is an obligation to store different types of documentation for a specific period.

Pursuant to Article 51.1 of the Act on National Archive Resources and Archives, in the event of liquidation or bankruptcy of an employer, such employer is required to indicate an entity conducting business activity in the field of documentation storage, to which his documentation will be transferred for further storage, and to provide the necessary funds till the end of a 50-year period of documentation storage, starting 1) on the day of the termination of work for such employer – for personal documentation; 2) on the day of its drawing up – for payroll documentation. In the event that a registry court states – on the request of the employer being subject to entry in the National Court Register or the register of business activity - that it is impossible to ensure the means for covering the expenses of further storage, the documentation shall be taken over by state archive, established for this purpose by the Minister of Culture and National Heritage. Before issuing a decision following such request, the court shall consult the head of the tax office having jurisdiction over the employer's seat about the employer's financial situation.

In connection with bankruptcy, it is possible to process personal data of indebted entrepreneurs in the insolvency register (maintained according to the Insolvency Act – No.182/2006 Coll.) which is publicly accessible, except for data specified in the Insolvency Act. If a debtor is a natural person, his name, surname, home address, birth number, or it does not exist, the date of birth are entered on the list of debtors; if it is a natural person with a registered seat pursuant to a special legal regulation, the seat is entered on the list of debtor as well. If the debtor is an entrepreneur, also a supplement identifying his company is entered on the list of debtors along with the place of his business (if different from his home address) and his company's identification number.
In all the above-mentioned cases, the data processing in terms of the Czech Data Protection Act is qualified as processing without the data subject's consent on the grounds that it is necessary to fulfil the controller's legal obligations.
In the case of termination of a business activity, the personal data of clients may be handled in two ways – they may be liquidated (erased) or, in accordance with the applicable law, transferred to another subject.

According to the Act, on winding-up the employment records have to be given to an administrator, who is a person appointed to keep such records.

4.2 Personal data processing in connection with employment

Processing of employees' data during the employment period

An employer is obligated to process his employees' personal data in a way and for as long as necessary for the purposes of human resources management. The detailed scope of data that

may be processed by the employer is regulated by specific legal acts of particular countries. Such scope covers the fields of social and health insurance as well as taxes in most countries.
When processing employees' data, the employers must be aware of the employees' rights to privacy protection at the workplace. Although the need to control the employees' work and to use the company's resources by employers shall be taken into account, the employers should remember that the employees also have specific rights.
In this chapter, we will focus on the scope of supervision techniques and methods that can be applied by employers in compliance with the provisions on data protection. Although the use of various supervision techniques may be justified by the special nature of work and business activity, the employer shall be obligated to inform the employees about the control mechanisms used in the company and the way they are implemented.

The legal basis for the processing of personal data of employees by an employer is provided by the Act of June 26th, 1974 - the Labour Code and its implementing secondary legislation, in particular, the Ordinance of the Minister of Labour and Social Policy of 28 May, 1996 on the Scope of Employers' Records in Matters Relating to Employment Relationship and the Keeping of Employees' Personal Files.
Employee information, such as their name and surname, or business e-mail address, are closely related to an employee's work and his performance. Therefore, such information may also be made publicly available by the employer even without the consent of the employee concerned. This is also confirmed by the Supreme Court decision of 19 November, 2003, ref. I PK 590/02, which states that "the surname and name is an outer hallmark of a natural person and its disclosure for the purpose of their identification generally can not be considered unlawful, unless it is done in combination with another violation of a personal interest, such as worship, privacy or personal dignity. Disclosure of the employee's surname (name) by an employer without his consent does not constitute an unlawful infringement of a personal interest, if it is warranted by the tasks and responsibilities of the employer related to running a business, is necessary and does not affect the rights and freedoms of the employee". Moreover, the Court in its judgment pointed out, that "the most important component of the employer (company) are people, and the operation of a business is inextricably linked with external contacts – partners, customers, (...). Therefore, an employer can not be prevented from disclosing the surnames of employees holding specific positions within the institution. The opposite position would lead to a paralysis or severe limitation of the employer's capacity, without any reasonable justification regarding the protection of employee rights and interests (...). The names and surnames of employees appear on the doors in the workplace, are placed on registered stamps, and documents prepared in connection with employment, presented in newsletters of institutions and enterprises, which means that according to common practice, they are essentially public".
The employer may also require other information or documents to verify an individual's entitlement to benefits from the social fund as provided for by the Act of 4 March 1994 on Employer's Social Fund and the Employer's By-laws. Pursuant to Article 8.1 of the above Law, the provision of reduced services and benefits and the amount of payments from the fund shall depend on daily circumstances, the family and the material situation of the person entitled to benefits. The terms and conditions of the use of services and benefits paid from the fund and the rules for allocating funds for specific purposes and the types of social activities should be defined by the employer's by-laws (Article 8.2).
The provisions cited above do not indicate exactly what information an employer may require from the employee in order to grant him social benefits from the capital fund. Therefore, in accordance

with the general rules, in order to allocate benefits from the social fund, the employer may require only such information about an employee which is adequate (necessary) for this purpose. Therefore, considering that the legislator provided only general guidelines regarding personal information that an employer may require from an employee for the purpose of granting him benefits from the social fund, such matters should be regulated in detail by the employer's by-laws.
With regard to the possibility of monitoring employees, such as their use of the Internet, checking their email correspondence, etc., such mechanisms have to be preceded by rules regulating the use of such technologies by employees as well as by prior notification of employees that such measure are in effect.
Work time control practices using biometric readers are prohibited.

In the case of permanent employment, employers are allowed, if not obliged to process certain data about their employees in a way, for periods, and with a quality determined by special legal regulations, or as necessary for the purposes of human resources management within the limits set by the Data Protection Act and the Labour Code, namely its Article 316(4).
From the viewpoint of special legal regulations, where the data processing may be grounded in the provisions of Articles (5)(2)(a) and (9)(d) of the Data Protection Act, it is necessary to emphasize that the extent of data to be processed by employers for specific purposes is very broad. On this account and the fact that these special provisions are frequently amended, it would have little sense to provide their complete list.
However, the following legal regulations which provide for the employer's obligation to process personal data for purposes stated therein are considered especially relevant:

a) Act No. 262/2006 Coll., Labour Code, as amended – e.g. Article 96 (registration of work hours, overtime work, night work, stand-by duty), Article 105 (records of work injuries and occupational diseases),
b) Act No. 187/2006 Coll., on Health Insurance, as amended,
c) Act No. 582/1991 Coll., on Organisation and Application of Social Security, as amended,
d) Act No. 48/1997 Coll., on Public Health Insurance, as amended,
e) Act No. 117/1995 Coll., on State Social Benefits, as amended,
f) Act No. 592/1992 Coll., on General Health Insurance Contributions, as amended,
g) Act No. 586/1992 Coll., on Income Tax, as amended,
h) Act No. 337/1992 Coll., on Administration of Taxes and Fees, as amended, alternatively Act No. 280/2009 Coll., the Tax Code.

These regulations apply mostly to taxation and social and health security. Moreover, there are also specific professional regulations authorizing employers to process personal data. For example, Act No. 49/1997 Coll., on Civil Aviation and the Amended Act No. 455/1991 Coll., on Trading (Trades Licensing Act), or Act No. 61/2000 Coll., on Sea Navigation, in the form of subsequent regulations or Act 114/1995 Coll., on Inland Navigation, as amended.
These legal regulations generally specify periods during which employers retain data. In the event that no period is provided, employers are allowed to keep the data in question for as long as any conceivable limitation periods, either subjective or objective, are running, as provided for in Article 333 of the Labour Code. The purposes for which data are kept may be different. One is the keeping of evidence in the event of possible disputes, or as proof against the authorities that relevant obligations have been met).
Regarding employment, it is important to say what the Labour Code in its Article 312 stipulates about personnel files. Pursuant to this Law employer is allowed to keep personal files on employees. A personnel file must contain only documents that are necessary for the

performance of work within the terms of employment. Only senior members of staff superior to the employee are allowed to examine such file. Officials of the Work Inspection Authority, Employment Authority, courts, the State Attorney's Office, the Police of the Czech Republic, the National Security Office and intelligence services are entitled to see the files. Employees have the right to look into their personnel files, to make excerpts or copies at the cost of their employer." Personnel files may also be kept pursuant to Article 5.2(a) and Article 9(d) of the Data Protection Act.

Employers are also allowed to insert into the personnel files, for example, alerts about work regulation breaches relating to the work performed by the employee (Article 52(g of the Labour Code).

Paragraphs 1 through 3 of Article 316 of the Labour Code provide that employees are not allowed to use the employer's production and working tools and equipment including IT and telecommunication devices for their personal needs without the employer's consent. Employers are allowed to supervise, in an appropriate manner, observance of this rule (Article 316.1 of the Labour Code). Furthermore, "employers are not allowed to interfere with the privacy of their employees without a serious reason ensuing from the special character of the employer's activity at workplaces and common areas of the employer in a way that they covertly or overtly monitor their employees, intercept and record their phone calls, read their electronic mails, or check deliveries addressed to an employee", (Article 316.2 of the Labour Code) However, "if employers have a serious reason stemming from the special character of the employer's activity which justifies implementation of control mechanisms pursuant to Article 2, they are obliged to inform directly their employees about the extent of such monitoring and how it is carried out", (Article 316.3 of the Labour Code). Along with this information obligation, employers are obliged to fulfil their obligations arising under the Data Protection Act, provided this law applies to such activity.

What kind of data can be processed about an employment relationship? According to the practise of the Data Protection Commissioner, it is against the Constitution when Article 77 of the Labour Code is applied during an employment relationship. The Labour Code does not rule this question, thus during an employment relationship new personal data can be processed only if the data subject has given his consent, based on Article 3. (3) of the DP&FOI Act.

Another important group of cases is how the employer may control the work of the employee and the use of work equipment.

1. *Surveillance systems*. There are two grounds for using surveillance systems in a workplace. The first is to guard equipment of high value, e.g. it is possible to use a camera in a warehouse. The other is to watch and check the intensity of the work of the employees. Surveillance system cannot be installed on this second ground, according to the practise of the Data Protection Commissioner. The case is different if the camera is not used for recording. This kind of surveillance system violates the personality rights of the persons concerned.
2. *Usage of e-mail box.* The employer may not check directly his employees' e-mail boxes, even if such e-mail boxes are used for work purposes only and the employer obtains the consent of the employee. The reason being that an mailbox may contain letters, which are protected by law since they could fall under the domain of the private sphere. If an employer would like to find out what the letters contain, he can ask the employee to show them to him, and the employee has the right not to disclose his private letters.
   On the other hand, the employer has the right to know directly the content of letters written by his employee. The reason for this is that the former Data Protection Commissioner was of the opinion that an employee has no influence on the content of incoming letters, only on the outgoing ones.
3. *Internet use*. It often happens that an employer wants to control the use of the Internet.

The Data Protection Commissioner emphasized in this case the principle of minimizing data: if the employer wants to limit the use of the Internet only to official purposes, then he should first limit visits only to those websites, which are needed for work. If this is not possible, he then can list the visited homepages.

4. *Computer*. It is important to note that the legal status of the computer as an object differs from the legal status of the data stored in the computer. It means that the employer has no right to know the data stored in the computer for work purposes. However, the case is different if data is stored in violation of the labour regulations.
5. *Telephone*. The use of telephones can generate high costs and the use for private purposes creates a tax obligation. That is why employers often want to check the use of telephone. According to the practise of the Data Protection Commissioner, it is unlawful to list the calls made by an employee or to eavesdrop or record them without the employee's consent.
6. *GPS localisation, mobile cell info*. One of the employee's basic obligations is to be where and when his employer orders him to do so. For this reason and to organise work, the employers regularly check the location of their employees by GPS or mobile cell info. According to the Data Protection Commissioner, these tools can be used only if it is really justified by work logistical grounds and such control can not be accomplished better by other tools. These tools may be used only during work hours.
7. *Information from the labour registers.* Employees often demand access to the labour registers e.g. the work hours register and meet with their employer's refusal. According to Article 12 of DP&FOI Act, such refusal is unlawful, unless it is permitted under an Act. This refusal violates the employer's right to self-determination in relation to information.

Personal data processing in connection with employment

Staff recruitment procedures are regulated by national legal provisions in each EU Member State. Selected issues in this field, in the context of personal data collection and processing are presented below.

Each country has enacted labour law provisions specifying in detail the scope of data which may be processed for this purpose. The scope of data which may be required from job applicants by employers depends on the nature of a work position and specific applicable provisions, if any.

The scope of personal data that an employer may collect from an employee and job applicant is regulated by Article 22^1 of the Act of 26 June 1974 - the Labour Code (Journal of Laws of 1998 No. 21, item 94, as amended). This provision was added under § 1 point 7 of the Act of 14 November 2003 amending the Act – the Labour Code and amendments to other acts (Journal of Laws No. 213, item 2081) and has been in force since 1 January 2004.

Pursuant to Article 22^1 § 1 of the Labour Code, the employer has the right to demand from the job applicant the following personal data: name(s) and surname, names of parents, date of birth, address of residence (correspondence address), information about his education and his employment history.

The scope of personal data which can be demanded by an employer from the employee is slightly broader. Paragraph 2 of the above-mentioned provision authorises the employer to demand other personal data about the employee, apart from the data listed in § 1, as well as names, surnames and dates of birth of his children, provided that such data are required if the employee is to benefit from special rights as provided for under the labour law, as well as the PESEL number (personal identification number) of the employee, assigned by the Common

Electronic System of Population Register (RCI PESEL). Moreover, the employer has the right to obtain from an employee other data than the ones mentioned above, if the obligation to provide the data arises under other legislative provisions (§ 4 of the above-quoted provision). Pursuant to Article 22^1 § 3 of the Labour Code, personal data are disclosed to the employer in the form of the data subject's declaration. The employer has the right to demand that the personal data of persons referred to in § 1 and 2 are documented.
It needs to be stressed that making such declaration by the job applicant or employee cannot be treated as giving consent to the processing of personal data of persons referred to in Article 23.1.1 of the Act on Personal Data Protection. Such consent is redundant, because the processing of personal data by the employer in the scope described above is conducted on the basis of a specific legal provision, where the prerequisite specified in Article 23.1.2 of the Act on Personal Data Protection is fulfilled.

The Labour Code (Act No. 262/2006 Coll.) determines certain limits of data processing. Employers are legally obligated to process certain data about employees, either current, former, or future, for different purposes, such as taxation or payment of social security and health contributions.
Primarily, it is important to realise that employment is nothing else than a contractual legal relation where the parties are formally equal.
In fact, the positions of subjects of employment contracts are rather unequal. This is to some extent compensated for by legal regulations in favour of the job applicant as the weaker party. At this stage, (the prospective) employer may require from the applicant personal information directly related to the conclusion of their employment contract.
It is not possible to compile a list of data that would meet the above criteria because their content depends on many variables, such as the nature of the work done, etc. In the event an employment relation is not established for some reason, employers should return to the job applicant all documents and data provided by him. Employers are allowed to continue collecting data only if the job applicant granted his consent on the prospect of possible future dealings relating to his employment (or for other purpose).

The legality of the questions asked during the admission procedure must be checked because the relationship between the candidate and the questioner is subordinate. In this case, the candidate has limited possibility of refusing to answer. According to Article 77 of the Act XXII of 1992 on the Labour Code (Labour Code), an employee shall only be requested to make a statement, fill in a data sheet, or take an aptitude test if it does not violate his personal rights and which essentially provides information considered substantive for the purposes of entering into an employment relationship. Employees must not be compelled to take a pregnancy test or to produce a certificate thereof, unless it is prescribed by the relevant legislation so in order to determine the employee's proficiency for the position in question.
Whenever an employee feels that the questions he is asked are not related to the employment relationship or his personality rights are limited or violated without reason, he has the right to gain information about the question and the data processing related to it and can put his questions to the questioner. The employee has the right to refuse to answer questions not related to a defined purpose according to DP&FOI Act and Article 77 of the Labour Code.
According to the purpose-bound nature of data processing, a person who was given the curriculum vitae by the employee can not hand it over to a third person, not even inform him

about the fact that the CV was submitted, unless the data subject has given his explicit consent. Various tools are used to check the ability of the employee during the admission procedure. The most widely used unlawful methods are related to measuring the personality of the candidate, in whole or in part, by psychological tests and the polygraph.
The polygraph was labelled clearly as unlawful by the Data Protection Commissioner in many positions. The psychological tests are considered unlawful, if the rights of the data subject are violated in the course of the procedure. Before filling in a psychological questionnaire, the data subject must be informed which questions will be answered by filling in the test and about the purpose of this kind of data processing. The person who analyses the test must also be named, because only he has the right to know the answers. After analysing a test, which measures the whole personality, the result must be communicated to the data subject. He has the right to decide whether the result can be transferred to the person in charge of the admission procedure. In the case of simpler questions, e.g. the capability of the employee, it is not necessary to obtain the consent of the person concerned, and the result can be transferred directly to the employer.

Termination of employment relationship

The employer should obey several rules which should not breach the former employees' privacy. The most important ones are the following:

– e-mail boxes must be deleted after termination of employment (the good practice is that the sender should get back the letters sent to a deleted email box with information about the deletion of the email box),
– the employee has the right to be informed for how long, by whom and for what purpose his/her personal data will be processed after termination of his employment,
– the contact data of the employee should be deleted from the employer's website.

The retention period of employees' data for the purpose of providing evidence of the employer's claims is the same as the statute of limitation for claims.

An employer is obligated to keep employee records for 50 years for social security purposes.

General statute of limitation is 3 years, but the objective statute of limitation for taxes is 10 years.

In Hungary the retention period of employees' data is three years.

4.3 Personal data in marketing and customer relations

Customers database

Although the legal provisions do not specify in detail which data should be collected from customers in order to perform a contract between an entrepreneur and a customer, such information shall not extend beyond the data necessary to identify a customer and to perform a contract. The scope of such information may differ depending on the nature and type of

services provided by the entrepreneur. There are, however, such types of contracts where the legal provisions clearly specify the scope of data required.
Upon concluding a contract, entrepreneurs collect their customers' personal data covered by the provisions on personal data. At the same time, data filing systems are created that include the data from such consumer contracts, in particular commodity sale contracts, lease contracts, insurance contracts, banking account contracts, electricity, water and gas supply contracts, as well as contracts for the provision of publicly available telecommunication services.
The entrepreneurs can, first of all, process the data collected in connection with the contracts concluded with customers for the purposes of performing these contracts and marketing their products and services.

The processing of data identifying the parties to a contract is especially important at the time such contract is concluded or performed. Basic information includes the name and surname, residence address, and more often the identity card number and PESEL number (personal identification number). However, one should always remember to collect data only in the scope necessary to perform a contract. Thus, excessive collection of data should be avoided.
The provisions very often directly indicate which data may be collected e.g. in relation to subscribers of telecommunication services. The provider of publicly available telecommunication services shall be entitled to process the following data on users who are natural persons: 1) names and surnames; 2) parents' names; 3) place and date of birth; 4) permanent residence address; 5) PESEL number (personal identification number) – in the case of a citizen of the Republic of Poland; 6) the name, series and number of documents proving identity, and in the case of a foreigner who is not a citizen of a Member State or the Swiss Confederation – passport number or residence card; 7) data contained in documents confirming the ability to perform an obligation towards the provider of publicly available telecommunication services resulting from the contract for the provision of telecommunication services. Apart from the data referred to above, the provider of publicly available telecommunication services can, upon the consent of a user who is a natural person, process other data from this user in relation to the provided service, in particular a tax identity number NIP, a bank account number or a payment card number, the user's correspondence address, if different from his permanent residence address, as well as an electronic mail address and contact telephone numbers.
It is important to remember that the processing of data for the purpose of performing a contract does not require the customer's consent.

The extent of personal data necessary for conclusion of written contractual relation between a company and its client as well as the performance thereof is practically defined by answering the following simple questions: who – to whom, what and for how much, when and how. The conclusion of contracts is generally based on the provisions of the Civil Code and the Commercial Code, or as the case may be, on other special laws. The law does not specify the extent of personal data necessary for identification of the party for most types of contracts. According to the Civil Code, in the process of concluding a contract all participants are obliged to remove all elements that could cause disputes. It is obvious that the basic prerequisite for avoiding arguments is the accuracy of personal data, especially in the case of written contracts. For the identification of a client as a party to a contract, the following information is most common: the name, surname, home address, and date of birth, if needed. This scope can be considered sufficient for all types

of written contracts, apart from those contracts where the law explicitly calls for the use of birth numbers as in the case of insurance contracts or contracts for the provision of publicly accessible services of electronic communication. If not explicitly required by law, birth numbers may be used only with the consent of its owners. Based on the type of the contract in question, the use of clients'identity card numbers may not be considered collection of data that does not meet the stated purpose. For example, in the case of accommodation contracts with hotels.
It is important to explain when the entering of personal data into a contract is classified as personal data processing. A single contract in its physical form cannot be regarded as processing of personal data of the contracting party in the meaning of the Data Protection Act. However, systematically concluded contracts with clients, e.g. for the sale of goods or provision of services shall be regarded as processing of personal data. The type of contract also carries implications for data processing operations of client data carried out during the performance of a contract. For instance, data files containing consumer contracts, especially sale contracts, lease contracts, insurance contracts, and the like, represent processing of personal data.
If client personal data are processed for the purpose of concluding and performing a contract to an appropriate extent and only for the purpose of delivery and invoicing of goods or services, then the data subject's consent is not required, pursuant to the exemption stated in Article 5.2(b) of the Data Protection Act.

There are no specific national variations.

Marketing activity

When offering products and services, the entrepreneurs use marketing techniques, like marketing materials that they send to their current and potential customers.
Direct marketing in EU Member States is regulated by various provisions. In particular, different principles may apply to the sending of marketing materials by regular mail or by electronic means. The use of personal data may be allowed under certain conditions without a previous consent of the customer – in such case, known as the „opt-out" principle, the customer must have the possibility to opt out of the services offered by the company (including marketing activities addressed to him/her) and may require that the processing of his/her personal data be stopped. In some instances, such consent is required.
Direct marketing carried out by electronic means must meet the requirements regarding the limitations on sending unsolicited correspondence (commercial spam). As a rule, sending commercial messages (e.g. advertisements) via the Internet should be allowed only with the expressed consent of the data subject (OPT-IN principle).

The Act of 29 August 1997 on the Protection of Personal Data determines when companies may send marketing offers to their customers. They can do this:

1. *without their consent* – in the case of marketing of one's own products or services. The legal basis for the use of their personal data shall be the legitimate interest of the controller (or company), referred to in Article 23.1.5 of the Act on Personal Data Protection. Pursuant to its provisions, the legitimate interest of the controller is the direct marketing of his own products or services. So, the data may be used for this purpose, provided that it does not violate the rights and freedoms of the data subject.

2. *with their consent* – in the case of marketing of other entity's products or services. There are no legal provisions which would permit sending a marketing offer of another entity as permissible on the grounds that it is in the controller's legitimate interest. Even concluding a contract of mutual marketing by both entities does not constitute a sufficient basis for stating that sending a marketing offer of the cooperating company is a legitimate interest of the controller.

For example, if a telecommunication operator, which concluded a cooperation agreement for the purpose of marketing his products with a bank, would like to send information on a beneficial bank loan to his customers, he would have to obtain their consent to do so. The information on a beneficial loan is the bank's marketing information, and not of the telecommunication operator. So, the telecommunication operator must obtain his customers' consent to be able to send them the bank's marketing offers.

In the event that the entrepreneur has bought a database for the purpose of marketing of his own products and services, he shall be obliged to previously inform the data subjects.

Pursuant to Article 25.1 of the Act of 29 August 1997 on the Protection of Personal Data in the event that the data have not been obtained from the data subject, the controller is obligated to provide the data subject, immediately after recording his/her personal data, with the following information: 1) the address of its seat and its full name (and in the case the controller is a natural person, about the address of his/her residence and his/her full name); the purpose and the scope of data collection, and in particular, about the data recipients; the source of data; the existence of the data subject's right of access to his/her data and the right to rectify these data, as well as the powers resulting from Article 32.1 points 7 and 8. The latter powers include the right to make a justified demand in writing for blocking the processing of his/her data, due to his/her particular situation (pt 7) and the right to object to the processing of his/her personal data (pt 8). Fulfilling the information obligation is connected with providing to the data subject certain information necessary for him to exercise his rights, e.g. the above right to object to the processing of his/her data or possible complaint against the controller.

Failure to fulfil the notification obligation as laid down in Article 25 of the Act is subject to criminal liability, because under Article 54 of the Act a person who, being the data controller, fails to inform the data subject of his rights or to provide him with the information which would enable that person to benefit from the provisions of this Act, shall be liable to a fine, partial restriction of freedom or imprisonment of up to one year. Let us refer to the Voivodeship Administrative Court in Warsaw judgment of 22 January, 2004 (file No. II SA 2665/2002) which reads "A company that acquired a personal data filing system from another data controller should notify customers that it is in possession of their data, and give them time to have a chance to object to the processing for marketing purposes. Failure to meet these conditions violates the provisions on data protection."

It is possible for a data subject to object to processing of his data in situations where the data controller processes his data for marketing purposes pursuant to Article 23.1.5 of the Act, which states that processing of data is permitted, inter alia, if processing is necessary for the purpose of legitimate interests pursued by the data controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject.

A data controller should stop further processing of personal data of a data subject in the event that the person objects to such processing. According to Article 32.3 of the Act, in the event that a data subject does file an objection, further processing is unacceptable.

However, the data controller is allowed to further process the name and surname of a person, as well as the address, serial number of the identify document or PESEL identification number in order to prevent the re-use of data for the purposes to which the data subject objected.

The right of every person to file an objection is linked with the responsibility of the data controller to apply such technical and organizational measures that would enable the immediate recording of such objection to further processing.

With regard to the sending of unsolicited electronic mail under the provisions of the Act on providing services by electronic means, which regulates issues concerning the obligations of service providers involved in providing electronic services and the protection of personal data of users of electronic mail, it is prohibited to transfer by means of electronic communication, in particular electronic mail, unsolicited commercial information addressed to a designated recipient (Article 10.1 of the above Act). Business information – pursuant to Article 10.2 of the above Act – is considered to be solicited, if the recipient has consented to receiving it, in particular, when he has provided his electronic mail address for this purpose. Article 4.1 of the above Act states that if a law requires the prior consent of the recipient, consent can not be alleged or presumed on the basis of a declaration of will of other content, and it may be revoked at any time. However, Article 10.3 of the above Act indicates that the transmission of unsolicited commercial information is an act of unfair competition in the meaning of the Act of 16 April 1993 on Counteracting Unfair Competition (Journal of Laws of 2003, No. 153, item 1503, as amended). In such cases, the person to whom the information in question is addressed may apply to the competent consumer protection advocate, having jurisdiction over his place of residence.

According to Czech legislation, the data protection authority is empowered to supervise compliance with Article 10 of the Certain Information Society Services Act (No. 480/2004 Coll.), as concerns certain services and the information obligation in relation to commercial information. The problem is that the law applies only to entities subject to Czech law, while the majority of spam is sent from abroad. The above-mentioned provisions do not apply to direct telephone calls. Pursuant to Act No. 127/2005 Coll., on electronic communications, it is prohibited to offer marketing advertisements or other similar products and services to persons who indicated in public phone books, issued pursuant to this law that they did not wish to be contacted for marketing purposes.

In Hungary, direct marketing is regulated in a number of legal instruments. Different rules apply to communication via traditional mail, electronic mail and by telephone; direct marketing conducted via traditional mail, electronic mail and by telephone. It is worthwhile to pay attention to the so-called Internet companies, which play a significant role in the market. It is not clear whether the Hungarian data protection and freedom of information act applies to such companies.

Data protection authorities involved in the project

POLAND

Bureau of the General for Personal Data Protection

The Inspector General for Personal Data Protection, established in 1998, is an independent supervisory authority with powers in the broad area of data protection. The responsibilities of the Inspector General for Personal Data Protection include: overseeing compliance of data processing with the Protection of Personal Data Law, issuing administrative decisions and considering complaints relating to the enforcement of the provisions on the protection of personal data, keeping a public register of data filing systems, issuing opinions on bills and regulations, participating in the work of international organisations and institutions involved in personal data protection, and last but not least, initiating and undertaking activities to improve the protection of personal data by publishing leaflets and other education activities.
The Inspector General has the authority to issue administrative decisions and consider complaints about the implementation of provisions on the protection of personal data.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Contact
ul. Stawki 2
00-193 Warszawa
Phone: (+48 22) 860 70 81
Fax: (+48 22) 860 70 90
E-mail: kancelaria@giodo.gov.pl
Website: www.giodo.gov.pl
Office hours: 8.00 – 16.00 Monday to Friday

THE CZECH REPUBLIC

Office for Personal Data Protection

Founded in June 2000, the Office for Personal Data Protection is an independent supervisory body vested with numerous competences. Its mission is to ensure that businesses and public authorities come to terms with the principles of data protection and to endeavour that individuals are aware of their rights ensuing from the data protection law. The Office's activities are manifold, ranging from handling complaints and investigations, consultancy and promotion to maintaining a register of notified processing operations, authorization of international data transfers, or preparation of positions on specific subject matters. Activities of the Office are governed by the Czech data protection law.

The Office is a respected player in the law-making process where it is involved as consultant always trying to promote the observance of the data protection requirements in the bills submitted by the government.

The Office offers to both professionals and the public advice and support and disseminates a number of valuable publications. Beside the regular Official Journal, Bulletin and Annual Report, readers may profit from different leaflets and brochures focused on interesting topics. The present guide, prepared jointly with the Polish and Hungarian partners is one of such publications.

úřad pro ochranu osobních údajů
the office for personal data protection

Contact
Pplk. Sochora 27
170 00 Prague 7
Phone: +420 234 665 111
Fax: +420 234 665 444
E-mail: posta@uoou.cz
Website: www.uoou.cz
Office hours: 7.30 – 16.15 Monday to Thursday
7.30 – 15.00 Friday

HUNGARY

Commissioner for Data Protection and Freedom of Information

The Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (DP&FOI Act) promulgated on 17 November 1992 provides for the establishment of a Commissioner for Data Protection and Freedom of Information to protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest. The Parliament appoints the Data Protection Commissioner; the institution was established on 30th June 1995.

The duties and scope of authority of the Commissioner are laid down by DP&FOI Act and other acts. The Data Protection Commissioner oversees compliance with the provisions of the data protection laws; investigate the reports (complaints) lodged with him and is responsible for keeping a data protection register. The Data Protection Commissioner facilitates uniform enforcement of the statutory provisions on the processing of personal data and on the availability of public information; and has authority to make general recommendations or those addressed to specific controllers. The Commissioner expresses his opinion concerning data made available to the general public and relating to the activities of state or local public authorities and agencies and other bodies attending to public duties specified by law. An important duty of the Commissioner is to give opinions on draft legislation concerning data protection and freedom of information and to make recommendations for new regulations.

The Data Protection Commissioner collaborates with bodies and persons specified by law to represent the Republic of Hungary in the European Union's common data protection supervisory bodies.

Upon noticing any unlawful data processing operation, the Data Protection Commissioner advises a data processor to cease such operation. If the controller or processor fails to comply, the Data Protection Commissioner may order, by resolution, the unlawfully processed data to be blocked, deleted or destroyed. The Data Protection Commissioner may announce to the general public the institution of proceedings, any illegitimate data management and may identify the controller (processor).

In addition to the duties determined by statutory instruments, the Commissioner has the responsibility to publicize and inform the public about the concept of data protection, its value to individual citizens, and their rights to freedom of information. This includes working with local and national media, publicizing legislation, marketing the services of the Commissioner and encouraging the development of teaching and research within the professional field. The present guide prepared jointly with the Polish and Czech partners represents this goal.

HUNGARIAN PARLIAMENTARY COMMISSIONER FOR
DATA PROTECTION AND FREEDOM OF INFORMATION

Contact
Nádor str. 22
1051 Budapest,
Mail: 1387 Budapest Po. box. 40
Phone: (+36 1) 475 7100
Fax: (+36 1) 269 3541
E-mail: adatved@obh.hu
Website: www.adatvedelmibiztos.hu