

# Consolidated version of the Personal Data Protection Act

Act No. 101/2000 Coll.,

of April 4, 2000

## on the Protection of Personal Data and on Amendment to Some Acts

as amended by the Act No. 227/2000 Coll., Act No. 177/2001 Coll., Act No. 450/2001 Coll., Act No. 107/2002 Coll., Act No. 310/2002 Coll., Act No. 517/2002 Coll., Act No. 439/2004 Coll., Act No. 480/2004 Coll., Act No. 626/2004 Coll., Act No. 413/2005 Coll., Act No. 444/2005 Coll., Act No. 109/2006 Coll., Act No. 112/2006 Coll., Act No. 342/2006 Coll., Act No. 170/2007 Coll., Act No. 41/2009 Coll., Act No. 52/2009 Coll., Act No. 227/2009 Coll., Act No. 281/2009 Coll. and Act No. 468/2011 Coll.

---

The Parliament has enacted the following Act of the Czech Republic:

### **Part One Personal Data Protection**

#### **Chapter I Introductory Provisions**

##### Article 1

##### **Subject of the Act**

This Act, in accordance with the law of the European Communities, international agreements binding the Czech Republic, and to exercise everyone's right to the protection from unauthorised interference with privacy, regulates the rights and obligations in processing of personal data and specifies the conditions under which personal data may be transferred to other countries.

##### Article 2

(1) The Office for Personal Data Protection is hereby established with seat in Prague (hereinafter referred to as the "Office").

(2) The Office shall be entrusted with the competence of a central administrative authority in the area of personal data protection in the scope provided by this Act and additional competences provided by special legal regulation, international treaties which form part of the legal order, and directly applicable law of the European Communities.

(3) The Office exercises the competence of a supervisory authority for the area of personal data protection following from international treaties which form part of the legal order.

##### Article 3

##### **Scope of the Act**

(1) This Act shall apply to personal data that are processed by state authorities, territorial self-administration bodies, other public authority bodies, as well as natural and legal persons.

(2) This Act shall apply to all personal data processing, both by automatic or other means.

(3) This Act shall not apply to personal data processing carried out by a natural person for personal needs exclusively.

(4) This Act shall not apply to accidental personal data collection, unless these data are subject to further processing.

(5) Furthermore, this Act shall apply to personal data processing:

(a) if the law of the Czech Republic is applicable preferentially on the basis of the international public law, even if the controller is not established on the territory of the Czech Republic,

(b) if the controller who is established outside the territory of the European Union carries out processing on the territory of the Czech Republic, unless where it is only the personal data transfer over the territory of the European Union. In this case the controller shall be obliged to authorize the processor on the territory of the Czech Republic under procedure laid down in Article 6.

If the controller carries out processing through its organization units established on the territory of the European Union, he must ensure that those organization units will process personal data in accordance with national law of a respective member state of the European Union.

(6) The provisions of Article 5(1) and Articles 11 and 12 of this Act shall not apply to processing of personal data necessary to fulfil obligations of the controller provided by special Acts to ensure:

(a) security of the Czech Republic,

(b) defence of the Czech Republic,

(c) public order and internal security,

(d) prevention, investigation, detection and prosecution of criminal offences,

(e) important economic interest of the Czech Republic or of the European Union,

(f) important financial interest of the Czech Republic or of the European Union, in particular the stability of financial market and currency, functioning of currency circulation and system of payments as well as budgetary and taxation measures, or

(g) exercise of control, supervision, surveillance and regulation related to exercise of public authority in the cases under (c), (d), (e) and (f), or

(h) activities related to disclosure of files of the former State Security.

#### Article 4

##### Definition of Terms

For the purposes of this Act:

(a) "personal data" shall mean any information relating to an identified or identifiable data subject. A data subject shall be considered identified or identifiable if it is possible to identify the data subject directly or indirectly in particular on the basis of a number, code or one or more factors specific to his/her physical, physiological, psychical, economic, cultural or social identity;

(b) "sensitive data" shall mean personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sexual life of the data subject and genetic data of the data subject; sensitive data shall also mean a biometric data permitting direct identification or authentication of the data subject;

(c) "anonymous data" shall mean such data that cannot be linked to an identified or identifiable data subject in their original form or following processing thereof;

(d) "data subject" shall mean a natural person to whom the personal data pertain;

(e) "personal data processing" shall mean any operation or set of operations that is systematically executed by a controller or a processor in relation to personal data by automatic or other means. Personal data processing shall mean, in particular, the collection of data, their storage on data carriers, disclosure, modification or alteration, retrieval, use, transfer, dissemination, publishing, preservation, exchange, sorting or combination, blocking and liquidation;

- (f) "personal data collection" shall mean a systematic procedure or set of procedures, which aim is to obtain personal data for the purpose of their further storage on a data carrier for their immediate or subsequent processing;
- (g) "personal data preserving" shall mean keeping data in a manner that permits their further processing;
- (h) „blocking“ shall mean any operation or set of operations that restrict the manner or means of personal data processing for a specified period of time, except for the necessary interventions;
- (i) "personal data liquidation" shall mean physical destruction of their carrier, their physical deletion or their permanent exclusion from further processing;
- (j) "controller" shall mean any entity that determines the purpose and means of personal data processing, carries out such processing and is responsible for such processing. The controller may empower or charge a processor to process personal data, unless a special Act provides otherwise;
- (k) "processor" shall mean any entity processing personal data on the basis of a special Act or authorisation by a controller;
- (l) "published personal data" shall mean personal data that are disclosed, in particular, by mass media, other form of public communication, or as a part of a public list;
- (m) "register or personal data file" (hereinafter referred to as "data file") shall mean any set of personal data that is structured or can be made available according to common or specific criteria;
- (n) "consent of data subject" shall mean a free and informed manifestation of will of the data subject the content of which is his assent to personal data processing;
- (o) "recipient" shall mean each subject to whom the personal data are disclosed. The subject processing personal data pursuant to Article 3(6)(g) is not considered a recipient.

## **Chapter II**

### **Rights and obligations in processing of personal data**

#### Article 5

- (1) The controller shall be obliged to:
- (a) specify the purpose for which personal data are to be processed;
- (b) specify the means and manner of personal data processing;
- (c) process only accurate personal data, which he obtained in accordance with this Act. If necessary, the controller is obliged to update the data. If the controller finds that the data being processed thereby are not accurate with respect to the specified purpose, he takes adequate measures without undue delays, in particular he blocks the processing and corrects or supplements the personal data, or otherwise he must liquidate the personal data. Inaccurate personal data may be processed only within the limits of the provisions of Article 3(6) of this Act. Inaccurate personal data must be branded. The controller is obliged to provide all the recipients with the information about blocking, correction, supplementing or liquidation of personal data without undue delay;
- (d) collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfilment of the specified purpose;
- (e) preserve personal data only for a period of time that is necessary for the purpose of their processing. After expiry of this period, personal data may be preserved only for purposes of the state statistical service, and for scientific and archival purposes. When using personal data for these purposes, it is necessary to respect the right to protection of private and personal life of the data subject from unauthorised interference and to make personal data anonymous as soon as possible;
- (f) process personal data only in accordance with the purpose for which the data were collected. Personal data may be processed for some other purpose only within the limits of the provisions of Article 3(6) or if the data subject granted his consent herewith in advance;

(g) collect personal data only in an open manner. Collecting data under the pretext of some other purpose or activity shall be prohibited;

(h) ensure that personal data that were obtained for different purposes are not grouped.

(2) The controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data:

(a) if he is carrying out processing which is essential to comply with legal obligation of the controller;

(b) if the processing is essential for fulfilment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the data subject;

(c) if it is essential for the protection of vitally important interests of the data subject. In this case, the consent of data subject must be obtained without undue delay. If the consent is not granted, the controller must terminate the processing and liquidate the data;

(d) 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, or

(e) 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 be in contradiction with the right of the data subject to protection of his private and personal life.

(f) if he provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity, their functional or working position, or

(g) if the processing relates exclusively to archival purposes pursuant to a special Act.

(3) If the controller processes personal data on the basis of a special Act, he shall be obliged to respect the right to protection of private and personal life of the data subject.

(4) When giving his consent the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. The controller must be able to prove the consent of data subject to personal data processing during the whole period of processing.

(5) If the controller or the processor carries out personal data processing for the purpose of offering business opportunities or services to the data subject, the data subject's name, surname and address may be used for this purpose provided that the data were acquired from a public list or in relation to his activity of controller or processor. The controller or processor, however, may not further process the data specified above if the data subject has expressed his disagreement therewith. The disagreement with processing must be expressed in writing. No additional personal data may be attached to the data specified above without the consent of data subject.

(6) The controller who process personal data pursuant to paragraph 5 may transfer these data to some other controller only if the following conditions are met:

(a) the data on the data subject were acquired in relation to activities of the controller or the data in question consist in published personal data;

(b) the data shall be used exclusively for the purpose of offering business opportunities and services;

(c) the data subject has been notified in advance of this procedure of the controller and the data subject has not expressed disagreement with this procedure.

(7) Other controller to whom data pursuant to paragraph 6 have been transferred may not transfer these data to any other person.

(8) Disagreement with processing pursuant to paragraph 6(c) must be expressed by the data subject in writing. The controller shall be obliged to notify each controller to whom he has transferred the name, surname and address of the data subject of the fact that the data subject has expressed disagreement with the processing.

(9) To eliminate the possibility that the name, surname and address of the data subject are repeatedly used for offering business opportunities and services, the controller shall be entitled to further process the subject's name, surname and address in spite of the fact that the data subject expressed his/her disagreement therewith in accordance with paragraph 5.

## Article 6

Where authorization does not follow from a legal regulation, the controller must conclude with the processor an agreement on personal data processing. The agreement must be made in writing. In particular, the agreement shall explicitly stipulate the scope, purpose and period of time for which it is concluded and must contain guarantees by the processor related to technical and organisational securing of the protection of personal data.

## Article 7

The obligations specified in Article 5 shall apply to the processor *mutatis mutandis*.

## Article 8

If the processor finds out that the controller breaches the obligations provided by this Act, the processor shall be obliged to notify the controller of this fact without delay and to terminate personal data processing. If he fails to do so, the processor and the data controller shall be liable jointly and severally for any damage incurred by the data subject. This shall in no way prejudice his responsibility pursuant to this Act.

## Article 9

### **Sensitive Data**

Sensitive data may be processed only:

(a) if the data subject has given his express consent to the processing. When giving his consent, the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. The controller must be able to prove the existence of the consent of data subject to personal data processing during the whole period of processing. The controller is obliged to instruct in advance the data subject of his rights pursuant to Articles 12 and 21,

(b) if it is necessary in order to preserve the life or health of the data subject or some other person or to eliminate imminent serious danger to their property, if his consent cannot be obtained, in particular, due to physical, mental or legal incapacity, or if the data subject is missing or for similar reasons. The controller shall be obliged to terminate data processing as soon as the above mentioned reasons cease to exist and must liquidate the data, unless the data subject gives his consent to further processing.

(c) if the processing in question is in relation with ensuring health care, public health protection, health insurance, and the exercise of public administration in the field of health sector pursuant to a special Act, or it is related to assessment of health in other cases provided by a special Act,

(d) if the processing is necessary to keep the obligations and rights of the controller responsible for processing in the fields of labour law and employment provided by a special Act,

(e) if the processing pursue political, philosophical, religious or trade-union aims and is carried out within the scope of legitimate activity of a civil association, foundation or other legal person of non-profit nature (hereinafter referred to as the "association"), and which relates only to members of the association or persons with whom the association is in recurrent contact related to legitimate activity of the association, and the personal data are not disclosed without the consent of data subject,

(f) if the data processed pursuant to a special Act are necessary to carry on sickness insurance, pension insurance (security), state social support and other state social security benefits, social services, social care, assistance in material need and social and legal protection of children, and if, at the same time, the protection of these data is ensured in accordance with the law,

(g) if the processing concerns personal data published by the data subject,

(h) if the processing is necessary to secure and exercise legal claims,

(ch) if they are processed exclusively for archival purposes pursuant to a special Act, or

(i) if it is the processing under special acts regulating prevention, investigation, detection of criminal activities, prosecution of criminal offences and search for persons.

## Article 10

In personal data processing, the controller and processor shall ensure that the rights of the data subject are not infringed upon, in particular, the right to preservation of human dignity, and shall also ensure that the private and personal life of the data subject is protected against unauthorized interference.

## Article 11

(1) In collecting personal data the controller shall be obliged to inform the data subject of the scope in which and the purpose for which the personal data shall be processed, who and in what manner will process the personal data and to whom the personal data may be disclosed, unless the data subject is already aware of this information. The controller must inform the data subject about his right of access to personal data, the right to have his personal data rectified as well as other rights provided for in Article 21.

(2) In case when the controller processes personal data obtained from the data subject, he is obliged to instruct the data subject on whether the provision of the personal data is obligatory or voluntary. If the data subject is obliged pursuant to a special Act to provide personal data for the processing, the controller shall instruct him on this fact as well as on the consequences of refusal to provide the personal data.

(3) The controller shall not be obliged to provide the information and instruction pursuant to paragraph 1 in cases where the personal data were not obtained from the data subject, if

(a) he is processing personal data exclusively for the purposes of state statistical service, scientific or archival purposes and the provision of such information would involve a disproportionate effort or inadequately high costs; or if storage on data carriers or disclosure is expressly provided by a special Act. In these cases the controller shall be obliged to take all necessary measures against unauthorised interference with the data subject's private and personal life.

(b) the personal data processing is imposed on him by a special Act or such data are necessary to exercise the rights and obligations ensuing from special Acts.

(c) he is processing exclusively lawfully published personal data, or

(d) he is processing personal data obtained with the consent of data subject.

(4) The above provisions shall be without prejudice to the rights of the data subject to request information pursuant to special Acts.

(5) In processing the personal data pursuant to Article 5(2)(e) and Article 9(h), the controller shall be obliged to inform without undue delay the data subject on processing of his personal data.

(6) No decision of the controller or processor in consequence of which is an interference with the legal and legally protected interests of the data subject, may not be issued or made without verification solely on the basis of automated personal data processing. This shall not apply where such decision was made in favour of the data subject and upon his request.

(7) The information obligation regulated by Article 11 may be performed by the processor on behalf of the controller.

## Article 12

### **Data subject's access to information**

(1) If the data subject requests information on the processing of his personal data, the controller shall be obliged to provide him with this information without undue delay.

(2) The contents of the information shall always report on:

(a) the purpose of personal data processing;

(b) the personal data or categories of personal data that are subject of processing including all available information on their source;

(c) the character of the automated processing in relation to its use for decision-making, if acts or decisions are taken on the basis of this processing the content of which is an interference with the data subject's rights and legitimate interests;

(d) the recipients or categories of recipients.

(3) For provision of this information the controller shall be entitled to require a reasonable reimbursement not exceeding the costs necessary for provision of information.

(4) The controller's obligation to provide the data subject with information pursuant to Article 12 may be met by a processor on behalf of the controller.

### **Obligations of Persons in Securing Personal Data**

#### Article 13

(1) The controller and the processor shall be obliged to adopt measures preventing unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data. This obligation shall remain valid after terminating personal data processing.

(2) The controller or the processor shall be obliged to develop and to document the technical-organisational measures adopted and implemented to ensure the personal data protection in accordance with the law and other legal regulations.

(3) In the framework of measures pursuant to paragraph (1), the controller or the processor perform a risk assessment concerning

(a) the carrying out of instructions for personal data processing by persons who have immediate access to the personal data,

(b) prevention of unauthorized persons' access to personal data and means for their processing,

(c) prevention of unauthorized reading, creating, copying, transferring, modifying or deleting of records containing personal data, and

(d) measures enabling to determine and verify to whom the personal data were transferred.

(4) In the area of automatic processing of personal data, the controller or processor shall, in the framework of measures under paragraph 1, be obliged to

(a) ensure that the systems for automatic processing of personal data are used only by authorized persons,

(b) ensure that the natural persons authorized to use systems for automatic processing of personal data have access only to the personal data corresponding to their authorization, and this on the basis of specific user authorizations established exclusively for these persons,

(c) make electronic records enabling to identify and verify when, by whom and for what reason the personal data were recorded or otherwise processed, and

(d) prevent any unauthorized access to data carriers.

#### Article 14

Employees of the controller or processor and other persons who process personal data on the basis of an agreement with the controller or processor, may process personal data only under the conditions and in the scope specified by the controller or the processor.

#### Article 15

(1) Employees of the controller or processor, other natural persons who process personal data on the basis of an agreement concluded with the controller or processor and other persons who, in the scope of fulfilling rights and obligations provided by law, come into contact with personal data at the premises of the controller or processor, shall be obliged to maintain confidentiality of personal data and security measures

whose publishing would endanger the security of personal data. The obligation to maintain confidentiality shall survive termination of employment or the relevant work.

(2) The provisions of the previous paragraph shall in no way prejudice the obligation to maintain confidentiality pursuant to special Acts.

(3) The obligation to maintain confidentiality shall not apply to information obligation pursuant to special Acts.

## Article 16

### Notification Obligation

(1) Whoever intends to process personal data as a controller or alter the registered processing pursuant to this Act, with the exception of the processing mentioned pursuant to Article 18, shall be obliged to notify in writing the Office of this fact prior to commencing personal data processing.

(2) The notification must include the following information:

(a) the identification data of the controller, i.e. in case of natural person who is not an entrepreneur his first name or names, surname, date of birth and address of permanent residence; in case of other subjects their trade, corporate or other name, seat and identification number if assigned, and name, eventually first names and surnames of persons that are their statutory representatives;

(b) the purpose or purposes of processing;

(c) the categories of data subjects and of personal data pertaining to these subjects;

(d) the sources of personal data;

(e) description of the manner of personal data processing;

(f) the location or locations of personal data processing;

(g) the recipient or category of recipients;

(h) the anticipated personal data transfers to other countries;

(i) the description of measures adopted for ensuring the protection of personal data pursuant to Article 13;

(3) If the notification includes all essentials pursuant to paragraph 2 and no proceeding pursuant to Article 17(1) has been initiated, the personal data processing may start after the expiration of 30 days from the delivery of the notification. In such case the Office records the information stated in the notification into the register.

(4) If the notification does not include all essentials pursuant to paragraph 2, the Office shall send without delay a reminder to the notifying subject in which he shall make reference to the missing or insufficient information and set a deadline for supplementing the notification. In case the notification is being supplemented, running of the time limit pursuant to paragraph 3 shall begin as of the day of delivery of the notification supplement. If the Office does not receive the notification supplement within the set deadline, the notification shall be regarded as if it has not been submitted.

(5) Upon the request from the controller the Office shall issue a certificate which includes date of issuance, reference number, first name, surname and signature of the person by whom the certificate has been issued, official stamp, identification data of the controller and purpose of processing.

(6) The Administrative Code shall not apply to the proceedings of the Office pursuant to paragraphs (1) - (5).

## Article 17

(1) If a justified concern arises in relation to the notification that this Act might be breached in processing of personal data, the Office shall initiate proceedings at its own instigation.

(2) If the Office finds that the controller does not breach by his notified processing the conditions specified by this Act, he shall suspend the proceedings and make a record pursuant to Article 16(3). The processing



of personal data may start not earlier than the day following the day when the record was made. In case the notified processing does not meet conditions specified by this Act, the Office shall not permit the processing of personal data.

#### Article 17a

(1) If the Office finds that the controller whose notification has been registered breaches the conditions provided by this Act, he shall decide on revocation of the registration.

(2) If the purpose for which the processing was registered ceases to exist, the Office shall decide on revocation of the registration either on its own instigation or on request of the controller.

#### Article 18

(1) The notification obligation pursuant to Article 16 shall not apply to processing of personal data:

(a) that are part of data files publicly accessible on the basis of a special Act,

(b) imposed on the controller by a special Act or when such personal data are needed for exercising rights and obligations following from a special Act, or

(c) in case of processing that pursues political, philosophical, religious or trade-union aims carried out within the scope of legitimate activity of an association and which relates only to members of the association or persons with whom the association is in recurrent contact related to legitimate activity of the association, and the personal data are not disclosed without the consent of data subject.

(2) The controller, who carries out processing pursuant to Article 18(1)(b), shall be obliged to ensure that the information concerning in particular the purpose of the processing, categories of personal data, categories of data subjects, categories of recipients and the period of preservation, which would otherwise be accessible by means of the register maintained by the Office pursuant to Article 35, is disclosed also through remote access or in other appropriate form.

#### Article 19

If the controller intends to terminate his activities, he shall be obliged to announce to the Office without delay how he handled personal data, if their processing is subject to the notification obligation.

#### Article 20

##### **Liquidation of Personal Data**

(1) The controller or, on the basis of his instructions, the processor shall be obligated to carry out liquidation of personal data as soon as the purpose for which personal data were processed ceases to exist or on the basis of a request by the data subject pursuant to Article 21.

(2) A special Act shall provide exceptions relating to the preservation of personal data for archival purposes and to the exercising of rights in civil judicial proceedings, criminal proceedings and administrative proceedings.

##### **Protection of Data Subjects' Rights**

#### Article 21

(1) Each data subject who finds or presumes that the controller or the processor is carrying out processing of his personal data which is in contradiction with the protection of private and personal life of the data subject or in contradiction with the law, in particular if the personal data are inaccurate regarding the purpose of their processing, he may:

(a) ask the controller or processor for explanation;

(b) require from the controller or processor to remedy the arisen state of affairs. It can mean in particular blocking, correction, supplementing or liquidation of personal data.

(2) If the requirement of the data subject pursuant to paragraph 1 is found justified, the controller or processor is obliged to remove without delay the improper state of affairs.

(3) If the data subject incurred other than property damage as a result of personal data processing, the procedure pursuant to a special Act shall be followed when lodging a claim.

(4) If a breach of obligations provided by law occurs in the course of processing of personal data by the controller or by the processor, they shall be liable jointly and severally.

(5) The controller shall be obliged to inform without undue delay the recipient on the requirement of the data subject pursuant to paragraph 1 and on the blocking, correction, supplementing or liquidation of personal data. This shall not apply where informing the recipient is impossible or would involve disproportionate effort.

Articles 22, 23 and 24 have been repealed.

#### Article 25

#### **Indemnification**

General regulation of liability for damage shall apply to matters not specified by this Act.

#### Article 26

The obligations pursuant to Articles 21 to 25 shall apply to persons who have collected personal data without authorisation *mutatis mutandis*.

### **Chapter III**

### **TRANSFER OF PERSONAL DATA TO OTHER COUNTRIES**

#### Article 27

(1) Free flow of personal data shall not be restricted if data are transferred to a member state of the European Union.

(2) Personal data may be transferred to third countries if the prohibition of restriction of the free movement of personal data is ensuing from an international treaty to the ratification of which the Parliament has given his assent and which is binding the Czech Republic, or if the personal data are transferred on the basis of decision of an institution of the European Union. The Office in the Official Journal publishes information about such decisions.

(3) Where the condition pursuant to paragraphs 1 and 2 is not met, the transfer of personal data may be carried out if the controller proves that:

(a) the data transfer is carried out with the consent of, or on the basis of an instruction by the data subject;

(b) in a third country, where personal data are to be processed, has been created sufficient specific guarantees for personal data protection, e.g. by other legal or professional regulations and security measures. Such guarantees may be specified in particular by a contract concluded between the controller and the recipient, if this contract ensures application of these requirements, or if the contract contains contractual clauses for personal data transfer to third countries published in the Official Journal of the Office;

(c) the personal data concerned are part of publicly accessible data files on the basis of a special Act or are, on the basis of a special Act accessible to someone who proves legal interest; in such case the personal data may be disclosed only in the scope and under conditions provided by a special Act;

(d) the transfer is necessary to exercise an important public interest following from a special Act or from an international treaty binding the Czech Republic;

(e) the transfer is necessary for negotiating the conclusion or change of a contract, carried out on the incentive of the data subject, or for the performance of a contract to which the data subject is a contracting party;

(f) the transfer is necessary to perform a contract between the controller and a third party, concluded in the interest of the data subject, or to exercise other legal claims, or

(g) the transfer is necessary for the protection of rights or important vital interests of the data subject, in particular for rescuing life or providing health care.

(4) Prior to the transfer of personal data to third countries pursuant to paragraph 3, the controller shall be obliged to apply to the Office for authorization to the transfer, unless provided otherwise by a special Act. When considering the application, the Office shall examine all circumstances related to the transfer of personal data, in particular the source, final destination and categories of personal data which are to be transferred, the purpose and period of the processing, with regard to available information about legal or other regulations governing the personal data processing in a third country. In the authorization to the transfer, the Office shall specify the period of time over which the controller may perform the data transfers. If a change of the conditions under which the authorization was issued occurs, in particular on the basis of a decision of an institution of the European Union, the Office shall alter or revoke this authorization.

#### **Chapter IV POSITION AND COMPETENCE OF THE OFFICE**

##### Article 28

(1) The Office is an independent body. In its activities, it shall act independently and shall observe only the Acts and other legal regulations.

(2) The activities of the Office may be intervened with only on the basis of law.

(3) The activities of the Office shall be paid for from a special chapter of the state budget of the Czech Republic.

##### Article 29

(1) The Office shall:

(a) perform supervision over the observance of the obligations provided by law in personal data processing;

(b) keep the register of personal data processing;

(c) accept incentives and complaints concerning breach of obligations provided by law in personal data processing and inform of their settlement;

(d) draw up an annual report on its activities and disclose the report to the general public;

(e) exercise other competence specified by law;

(f) discuss misdemeanours and other administrative offences and impose fines pursuant to this Act;

(g) ensure fulfilment of requirements following from international treaties binding the Czech Republic, and directly applicable law of the European Communities,

(h) provide consultations in the area of personal data protection,

(i) co-operate with similar authorities in other countries, with institutions of the European Union and with bodies of international organizations operating in the area of personal data protection. In accordance with the law of the European Communities the Office meets the obligation of notification towards the institutions of the European Union.

(2) Supervision in the form of inspection shall be performed pursuant to a special Act.

(3) Supervision over personal data processing performed by intelligence services shall be regulated by a special Act.

#### Article 29a

(1) The Ministry of Interior or the Police of the Czech Republic shall provide the Office for executing its competence pursuant to this Act and other legal regulations

- a) reference data from the basic register of population,
- b) data from the service-related population information system
- c) data from the service-related foreigners information system

(2) Data provided pursuant to paragraph (1)(a) are:

- a) surname,
- b) name or names,
- c) address of residence,
- d) date of birth.

(3) Data provided pursuant to paragraph (1)(b) are

- a) name or names, surname and name at birth if applicable,
- b) date of birth,
- c) address of permanent residence including previous addresses of permanent residence, d) commencement of permanent residence or date of annulment of permanent residence, or date of termination of permanent residence on the territory of the Czech Republic.

(4) Data provided pursuant to paragraph (1)(c) are

- a) name or names, surname and name at birth if applicable,
- b) date of birth,
- c) type of residence and address of residence,
- d) number and validity of the residence permit,
- e) commencement of residence or date of its termination if applicable.

(5) Data kept as reference data in the basic register of population may be collected from the service-related population information system or service-related foreigners information system only if they are in a format preceding the current state.

(6) Of the data provided only those data deemed necessary for satisfaction of a given task may be used in a particular case.

### **Chapter V ORGANISATION OF THE OFFICE**

#### Article 30

(1) Employees of the Office shall consist in the President, inspectors and other employees.

(2) Control activities of the Office shall be carried out by inspectors and authorised employees (hereinafter referred to as "the controlling persons").

(3) The provisions of the Labour Code shall apply to the employees of the Office, unless this Act provides otherwise.

(4) The President of the Office shall have the right to a salary, reimbursement of expenses and consideration in kind as the President of the Supreme Audit Office pursuant to a special Act.

(5) The inspectors of the Office shall have the right to a salary, reimbursement of expenses and consideration in kind as the members of the Supreme Audit Office pursuant to a special Act.

#### Article 31

Control activities of the Office shall be performed on the basis of a control plan or on the basis of the incentives and complaints.

#### Article 32

##### **President of the Office**

(1) The Office is directed by the President who shall be appointed and recalled by the President of the Czech Republic on the basis of a proposal of the Senate of the Parliament of the Czech Republic.

(2) The President of the Office shall be appointed for a period of 5 years. The President may be appointed for the maximum of two successive periods.

(3) The President of the Office may be only a citizen of the Czech Republic who:

(a) enjoys legal capacity,

(b) is impeccable, meets the conditions prescribed by a special regulation and for whom it can be assumed in relation to his knowledge, experience and moral qualities that he will serve his position properly,

(c) has completed university education.

(4) For the purpose of this Act, a natural person shall be considered impeccable if he has not been lawfully sentenced for a wilful criminal offence or for an offence committed by negligence in relation to personal data processing.

(5) The position of the President of the Office shall not be compatible with the positions of a Member of the Parliament or Senator, judge, state attorney, any position in the state administration, a position of a member of a territorial self-administration body and with the membership in political parties and movements.

(6) The President of the Office may not hold any other paid position, be in some other labour relationship, or perform any gainful activity, with the exception of administration of his own property and scientific, pedagogical, literary, journalistic and artistic activities, if such activities do not impair the dignity of the Office or threaten confidence in the independence and impartiality of the Office.

(7) The President of the Office shall be recalled from his position if he ceases to meet any of the conditions for his appointment.

(8) The President of the Office may also be recalled from his position if he fails to perform his position for a period of 6 months.

##### **Inspectors of the Office**

#### Article 33

(1) An inspector shall be appointed and recalled by the President of the Czech Republic on the basis of a proposal of the Senate of the Parliament of the Czech Republic.

(2) An inspector shall be appointed for a period of 10 years. He may be appointed repeatedly.

(3) An inspector shall carry out inspections, direct inspections, prepare the inspection report and perform other acts related to tasks of the Office.

(4) The activities pursuant to paragraph 3 shall be carried out by 7 inspectors of the Office.

#### Article 34

(1) An inspector may be only a citizen of the Czech Republic who enjoys legal capacity, has no criminal record, meets the conditions prescribed by a special legal regulation and has completed professional university education.

(2) The position of an inspector shall not be compatible with the positions of a Member of Parliament or Senator, judge, state attorney, any position in the state administration, a position of a member of a territorial self-administration body and membership in political parties and movements. An inspector may not hold any other paid position, be in some other labour relationship, or perform any gainful activity, with the exception of administration of his own property and scientific, pedagogical, literary, journalistic and artistic activities, if such activity does not impair the dignity of the Office or threaten confidence in the independence and impartiality of the Office.

(3) An inspector shall be recalled from his position if he ceases to meet any of the conditions for his appointment.

### **Chapter VI ACTIVITIES OF THE OFFICE**

#### Article 35

##### **Register**

(1) Information following from notifications pursuant to Article 16(2) and the date of execution or cancellation of the registration shall be recorded beside the entities of controllers in the Register of permitted personal data processing.

(2) Information written into the register, except the information referred to in Article 16(2)(e) and (i), are publicly accessible especially in the manner enabling remote access.

(3) Cancellation of registration pursuant to Article 17(a) shall be notified by the Office in the Official Journal of the Office.

#### Article 36

##### **Annual Report**

(1) The annual report of the Office shall include, in particular, information on the performed control activities and evaluation thereof, information on and evaluation of the state of affairs in the area of processing and protection of personal data in the Czech Republic and evaluation of other activities of the Office.

(2) The President of the Office shall submit the annual report for information purposes to the Chamber of the Deputies and the Senate of the Parliament of the Czech Republic and to the Government of the Czech Republic within 2 months of the end of the budgetary year, and it shall be published.

#### Article 37

##### **Rights of the Controlling Persons**

When performing inspection, the controlling persons shall be entitled to:

(a) enter the premises, facilities and plants, properties and other premises of the controllers and processors, who are subjected to inspection, or every person who processes personal data (hereinafter referred to as the "controlled person"), if this is related to the subject of the inspection; the controlling persons may enter dwellings only if the relevant dwelling serves also for operation of business activities;

(b) require that the controlled person and other persons submit within the specified deadlines original documents and other written materials, data records on computer-readable media, excerpts and software source codes, if these materials are owned thereby, excerpts and copies of data (hereinafter referred to as the "documents"), provided that these documents are related to the subject of inspection, and draw up their own documentation;

- (c) get acquainted with classified information under the conditions provided by a special regulation, as well as with other information that is protected by the obligation to maintain confidentiality;
- (d) request that natural and/or legal persons provide authentic and complete information of the determined and related facts;
- (e) seize documents in justified cases; the act of taking over the documents must be confirmed in writing to the controlled person, and on his request, he must be provided with copies of the seized documents;
- (f) make copies of the content of computer-readable media found at the premises of the controlled person that contain personal data;
- (g) request that the controlled persons submit within the set deadline a written report on a remedy of any shortcomings found;
- (h) use telecommunication facilities of the controlled persons in cases where use thereof is essential for ensuring the inspection.

## Article 38

### **Obligations of the Controlling Persons**

- (1) Controlling persons, in connection to whom reasonable doubts exist as to their prejudice with respect to their relationship with controlled persons or the subject of control, may not carry out inspections.
- (2) Immediately after learning facts indicating his prejudice, a controlling person shall be obliged to notify the President of the Office of this fact.
- (3) The President of the Office shall make a decision on an objection concerning prejudice of the controlled person without undue delay. Prior to making a decision on the objection concerning prejudice, the controlling person shall carry out only acts that cannot be delayed.
- (4) A decision on an objection concerning prejudice shall not be subject to appeal.
- (5) The controlling persons shall be obliged to:
  - (a) identify themselves to the controlled person by a document the model of which shall be specified by a decree of the Government;
  - (b) notify the controlled person of commencement of inspection;
  - (c) respect the rights and legally protected interests of controlled persons;
  - (d) return the seized documents and copies of computer-readable media to the controlled person as soon as the reasons for their seizure cease to exist;
  - (e) duly protect the seized documents against loss, destruction, damage or misuse;
  - (f) draw up an inspection report on the results of inspection;
  - (g) maintain confidentiality of facts found during the inspection and not to misuse knowledge of these facts. The obligation to maintain confidentiality shall not prejudice the notification obligation pursuant to special Acts. The obligation to maintain confidentiality shall survive the termination of the labour relationship with the Office. The President of the Office may release the controlling person from the obligation to maintain confidentiality. The obligation to maintain confidentiality shall not apply to anonymous and generalised information.
- (6) The inspection report shall include description of the established facts, together with specification of shortcomings and identification of provisions of legal regulations that have been breached and measures that were imposed for a remedy and setting of deadlines for providing for a remedy. The inspection report shall include designation of the Office and the names of the controlling persons participating in the inspection, designation of the controlled person, the place and time of performing the inspection, the subject of the inspection, the actual state of affairs, identification of documents and other documents and the findings on which the report is based. The inspection report shall be signed by the controlling persons who participated in the inspection.

(7) The controlling persons shall be obliged to acquaint the controlled persons with the contents of the inspection report and provide them with a copy thereof. The controlled persons shall confirm their acquaintance with the inspection report and takeover thereof by signing the inspection report. If the controlled person refuses to be acquainted with the contents of the inspection report or to confirm the acquaintance, these facts shall be stated in the inspection report.

#### Article 39

(1) In relation to performance of an inspection, each person shall be obliged to provide the required co-operation to the controlling persons in performance of their activities.

(2) A disciplinary fine up to CZK 25,000 may be imposed, even repeatedly, on a person who fails to provide the Office with the required co-operation in performance of an inspection. Even a default in adopting measures imposed for elimination of established facts within the prescribed deadline is considered as a failure to provide co-operation.

### Measures for Remedy

#### Article 40

(1) If a controlling person finds that obligations imposed by this Act have been breached, the inspector shall determine which measures shall be adopted in order to eliminate the established shortcomings and set a deadline for their elimination.

(2) If liquidation of personal data has been ordered, the relevant personal data shall be blocked until their liquidation. The controller may submit an objection to the President of the Office against ordering of the liquidation. The personal data must stay blocked until a decision on the objection is made. A legal action may be taken against the decision of the President according to the regulations on administrative justice. The data stay blocked until a decision is made by the court.

(3) The controlled person shall be obliged to submit a report on the adopted measures within the set deadline.

#### Article 41

Unless a provision of this Act provides otherwise, the Administrative Code shall govern proceedings in matters regulated by this Act.

#### Article 42

Operation of information systems managing personal data according to current regulations shall mean personal data processing.

#### Article 43

### Rights and Obligations in Supervision

The rights and obligations of controlling and controlled persons shall be governed by a special Act, unless this Act provides otherwise.

## Chapter VII ADMINISTRATIVE DELICTS

#### Article 44

(1) Natural person who

(a) is in a labour or similar relationship to the controller or processor;



(b) carries out activities for the controller or processor on the basis of an agreement, or who  
(c) in the framework of fulfilling powers and obligations imposed by a special Act comes into contact with personal data at the controller or processor,  
has committed an offence by breaching the obligation to maintain confidentiality (Article 15).

(2) Natural person in the position of the controller or processor commits an offence in the course of personal data processing if he:

(a) fails to specify the purpose, means or manner of processing (Article 5(1)(a) and (b)) or breaches an obligation by the specified purpose of processing or exceeds his authority ensuing from a special Act,

(b) processes inaccurate personal data (Article 5(1)(c))

(c) collects or processes personal data in a scope or manner which does not correspond to the specified purpose (Article 5(1)(d),(f) thru (h))

(d) preserves personal data for a period longer than necessary for the purpose of processing (Article 5(1)(e))

(e) processes personal data without the consent of data subject except the cases provided by law (Article 5(2) and Article 9)

(f) fails to provide the data subject with information in the scope or in the manner provided by law (Article 11)

(g) refuses to provide the data subject with the requested information (Articles 12 and 21)

(h) fails to adopt or implement measures for ensuring security of personal data processing (Article 13)

(i) fails to fulfil the notification obligation pursuant to this Act (Articles 16 and 27)

(3) Natural person in the position of the controller or processor commits an offence if he in the course of personal data processing:

(a) jeopardises a substantial number of persons by unauthorized interference in the private and personal life, or

(b) fails to fulfil obligations related to the processing of sensitive data (Article 9)

by some of the courses of action pursuant to paragraph 2.

(4) A fine up to CZK 100,000 may be imposed for an offence pursuant to paragraph 1.

(5) A fine up to CZK 1,000,000 may be imposed for an offence pursuant to paragraph 2.

(6) A fine up to CZK 5,000,000 may be imposed for an offence pursuant to paragraph 3.

#### Article 44a

(1) Natural person commits an offence by breaching prohibition of publishing of personal data provided by other legal regulation.

(2) A fine up to CZK 1,000,000 may be imposed for an offence pursuant to paragraph 1.

(3) A fine up to CZK 5,000,000 may be imposed for an offence pursuant to paragraph 1 committed by press, film, radio, television, computer network opened to the public or by other equally effective way.

#### Article 45

(1) Legal or natural person carrying on business according to special regulations when processing personal data in the position of the controller or processor commits an administrative delict if he:

(a) fails to specify the purpose, means or manner of processing (Article 5(1)(a) and (b)) or breaches an obligation by the specified purpose of processing or exceeds his authority ensuing from a special Act;

- (b) processes inaccurate personal data (Article 5(1)(c));
  - (c) collects or processes personal data in a scope or manner which does not correspond to the specified purpose (Article 5(1)(d), (f) thru (h));
  - (d) preserves personal data for a period longer than necessary for the purpose of processing (Article 5(1)(e));
  - (e) processes personal data without the consent of data subject, except the cases provided by law (Article 5(2) and Article 9);
  - (f) fails to provide the data subject with information in the scope or in the manner provided by law (Article 11);
  - (g) refuses to provide the data subject with the requested information (Article 12 and Article 21);
  - (h) fails to adopt or implement measures for ensuring security of personal data processing (Article 13);
  - (i) fails to fulfil the notification obligation pursuant to this Act (Articles 16 and 27);
  - (j) don't maintain an inventory of personal data breaches pursuant to Article 88 (7) of the Electronic Communications Act.
- (2) Legal person in the position of the controller or processor commits an administrative delict if he in the course of personal data processing:
- (a) jeopardises a substantial number of persons by unauthorized interference in the private and personal life, or
  - (b) fails to fulfil obligations related to the processing of sensitive data (Article 9)
- by some of the courses of action pursuant to paragraph 1.
- (3) A fine up to CZK 5,000,000 shall be imposed for an administrative offence pursuant to paragraph 1.
- (4) A fine up to CZK 10,000,000 shall be imposed for an administrative offence pursuant to paragraph 2.

#### Article 45a

- (1) Legal person or natural person doing business commits an administrative delict by breaching prohibition of publishing of personal data provided by other legal regulation.
- (2) A fine up to CZK 1,000,000 shall be imposed for an administrative delict pursuant to paragraph 1.
- (3) A fine up to CZK 5,000,000 shall be imposed for an offence pursuant to paragraph 1 committed by press, film, radio, television, computer network opened to the public or by other equally effective way.

#### Article 46

- (1) Legal person shall not be liable for an administrative delict if he proves that he has made best efforts reasonable to be required to prevent the breach of a legal obligation.
- (2) When deciding on the amount of the fine, especially the seriousness, manner, duration and consequences of the unlawful behaviour and the circumstances under which the unlawful behaviour was committed shall be taken into account.
- (3) Liability of the legal person for an administrative delict becomes extinct, if the administrative body has not initiated proceedings within 1 year as of the day when it learned of it, but not later than within 3 years as of the day when the delict was committed.
- (4) Administrative delicts pursuant to this act shall be dealt with in the first instance by the Office.
- (5) The provisions on the liability of legal person and related sanctions applies on the liability for the behaviour of natural person that occurred when the natural person carried on business activities or in a direct relation to such business activities.
- (6) The fine is payable within 30 days as of the day when the decision on imposing the fine came into force.

(7) The fine shall be collected by the Office. The revenue from fines shall be an income of the state budget.

**Chapter VIII  
COMMON, TRANSITIONAL AND FINAL PROVISIONS**

Article 47

**Measures for the Transitional Period**

(1) Every person who processes personal data by the date of entry into effect of this Act and who is subject to the notification obligation pursuant to Article 16 shall be obliged to fulfil this obligation at the latest within 6 months as of the date of entry into effect of this Act.

(2) Personal data processing carried out prior to the date of entry into effect of this Act shall be brought into accordance with this Act by December 31, 2001.

(3) In case the controlling persons establish a breach of obligations pursuant to paragraph 2, the provisions of Article 46(1) and (2) shall not be applied in such case prior to December 31, 2002

Article 48

**Repealing Provision**

Act No. 256/1992 Coll., on the Protection of the Personal Data in Information Systems is hereby repealed.

**Part TWO**

Repealed

Article 49

Repealed

**Part THREE**

Article 50

**Amendment to the Act on Free Access to Information**

Act No. 106/1999 Coll., on Free Access to Information, shall be amended as follows:

1. Article 2 paragraph (3), including footnote No.1 shall read:

"(3) The Act shall not apply to the provision of personal data and information pursuant to a special regulation.<sup>1</sup>

---

<sup>1</sup>E.g., Act No. 101/2000 Coll., on the Protection of Personal Data and Amendment to Some Related Acts and Act No. 123/1998 Coll., on the Right to Information on the Environment."

In article 5 paragraph (3), the second sentence shall be replaced by a sentence which, including the footnote No. 3a, shall read: "For this purpose, the obligation to avoid combining information pursuant to a special regulation shall not apply to these entities.<sup>3a</sup>

---

<sup>3a</sup> Article 5 (1) (h) of Act No. 101/2000 Coll., on the Protection of Personal Data and Amendment to Some Acts".

3. In Article 8, paragraphs (1) and (2), including the heading and footnote No. 5, shall be repealed.

**Part FOUR**  
**Legal Force**

Article 51

This Act comes into effect on June 1, 2000, with the exception of the provisions of Articles 16, 17 and 35, which come into effect on December 1, 2000.

(signed)

Article II

Transitional provisions of Article II of the Act No. 439/2004 Coll.

1. Notifications and decisions on the registration of personal data processing pursuant to Articles 16, 17 and 17a of the Act No. 101/2000 Coll., on the Protection of Personal Data and on Amendment to Some Acts in wording of the Act No. 450/2001 Coll., submitted and issued prior to the day of entry into effect of this Act continue to be valid.
2. Permissions for transfer or transfers of personal data to other state issued prior the day of entry into effect of this Act shall cease to have force on the day of entry into effect of this Act, if the state for which this permission was meant is a member state of the European Union or a state for which the prohibition to restrict the free movement of personal data ensues from a published international agreement, to the ratification of which the Parliament has given his assent and which is binding the Czech Republic. Permissions to transfer or transfers of personal data to a state not mentioned in the proceeding sentence issued before the Act has come into effect continue to be valid.
3. Proceedings initiated and not terminated before the effective date of Act shall be completed pursuant to applicable legal regulations except of proceedings on the permission for transfer or transfers of personal data to a member state of the European Union or a state for which the prohibition to restrict the free movement of personal data ensues from a published international agreement, to the ratification of which the Parliament has given his assent and which is binding the Czech Republic, that will be discontinued.
4. A controller performing the personal data processing for which no registration was needed pursuant to previous legal regulations and which underlies registration as of the day of entry into effect of this Act must notify such personal data processing to the Office for Personal Data Protection within 6 months as of the day of entry into effect of this Act.