

NATIONAL COUNCIL OF THE SLOVAK REPUBLIC



**Act No. 428/2002 Coll. on Protection of Personal Data,
as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll.
and the Act No. 90/2005 Coll.**

F U L L W O R D I N G

The National Council of the Slovak Republic has approved the following Act:

P A R T O N E

BASIC PROVISIONS

Object and Operation

Section 1

(1) This Act regulates

- a) protection of personal data of natural persons in the course of their processing,
- b) principles of personal data processing,
- c) security of personal data,
- d) protection of the rights of data subjects,
- e) transborder personal data flow,
- f) registration and keeping of records of filing systems,
- g) establishment, status and scope of powers of the Office for Personal Data Protection of the Slovak Republic (hereinafter the “Office”).

(2) This Act applies to the state administration authorities, territorial self-government authorities, other public authority bodies, as well as to other legal and natural persons, which process personal data, determine the purpose and means of processing or provide personal data for their processing.

(3) This Act also applies to the controllers, which do not have their registered office or permanent residence on the territory of

- a) the Slovak Republic but are located abroad at a place, where the laws of the Slovak Republic take precedence based on an international public law,
- b) a Member State of the European Union, provided that for the purposes of personal data processing they use fully or partially automated means or other than automated means of processing located on the territory of the Slovak Republic, while such means of processing are not used solely for the transfer of personal data through the territory of the Member States of the European Union; in such case the controller shall proceed pursuant to Section 23a Paragraph 3.

(4) This Act applies to the personal data systematically processed by fully or partially automated means of processing or by other than automated means of processing, which constitute a part of a filing system or are intended for processing in a filing system.

Section 2

(1) Provisions of Section 5 Paragraph 4, Section 6 Paragraphs 1 to 4, Section 10 Paragraphs 1, 2 and 8, Section 20 Paragraph 1, Section 27 and Section 32 shall not apply to the processing of personal data necessary for safeguarding of the public interest, provided that the controller fulfils the obligations expressly stipulated by a special Act determined for safeguarding of

- a) security of the Slovak Republic,
- b) defence of the Slovak Republic,
- c) public policy and security,
- d) preventing, precluding, detecting and documenting of criminal offences, disclosing their perpetrators, investigating and prosecuting of criminal offences,
- e) important economic or financial interests of the Slovak Republic or of the European Union, including monetary, budgetary and taxation matters,
- f) inspection, internal supervision, external supervision or regulatory function connected with exercise of official authority in cases referred to in Subparagraphs c), d) and e), or
- g) protection of the data subject or of the rights and freedoms of others.

(2) Only a State authority established by a special Act¹⁾ may act as the controller of a register of persons sentenced by a final decision delivered by courts in the criminal proceedings, or of a register of persons against which a prosecutor or court delivered a final decision on conditional discontinuation of criminal prosecution or on approval of a conciliation.

Section 2a

This Act shall not apply to protection of personal data

- a) processed by the natural person for his own needs within the framework of purely personal or household activities, like keeping a personal directory or correspondence,

¹⁾ E.g. Section 40 Paragraph 2 Subparagraph d) of the Act No. 153/2001 Coll., Act No. 311/1999 Coll. on Criminal Register, as amended.

- b) which were obtained accidentally without prior determination of the purpose and means of processing, without the intent of their further processing in an organized system according to special criteria and which are not further systematically processed.

Definition of Terms

Section 3

Personal Data

Personal data shall mean any information relating to an identified or identifiable natural person, while such person is one who can be identified, directly or indirectly, in particular by reference to a identifier of general application or by reference to one or more factors specific to his physical, physiological, psychic, mental, economic, cultural or social identity.

Section 4

(1) For the purposes of this Act:

- a) processing of personal data shall mean any operation or set of operations which is performed upon personal data such as obtaining, collection, recording, organization, adaptation or alteration, retrieval, consultation, alignment, combination, transfer, use, storage, destruction, transmission, provision, making available or making public,
- b) provision of personal data shall mean submitting of personal data for their processing to another controller or to the controller's representative or his processor,
- c) making personal data available shall mean disclosing of personal data or making them available to another legal or natural person, except for the data subject or the entitled person, who will not process them like a controller, controller's representative or processor,
- d) making personal data public shall mean publication or displaying of personal data in public by means of the mass media, publicly accessible computer networks, creating or exhibiting a piece of work in public,²⁾ public announcement, presenting on a public list, register or file,³⁾ their placing on an official board or other publicly accessible place,
- e) destruction of personal data shall mean liquidation of personal data by breaking them down, erasing them or by physically destroying material carriers in the manner precluding reproduction of the personal data,
- f) blocking of personal data shall mean putting personal data in such state, in which they are not available and any handling is precluded,

²⁾ Section 13 of the Act No. 383/1997 Coll., Copyright Act and the Act Changing and Amending the Customs Act, as amended.

³⁾ E.g. Sections 27 to 34 of the Commercial Code, Sections 8 and 68 of the Act of the National Council of the Slovak Republic No. 162/1995 Coll. on Land Registry and Registration of Ownership and Other Rights to Immovable Assets (Land Registry Act), as amended by the Act No. 255/2001 Coll., Section 26 Paragraph 2 Subparagraph e) of the Act No. 195/2000 Coll. on Telecommunications.

- g) filing system shall mean any structured set, system or database containing one or more personal data, which are systematically processed for the needs of achieving the purpose according to specific criteria and conditions, while using automated, partially automated or other than automated means of processing, disregarding the fact whether the system is centralised, decentralized or dispersed on a functional or geographical basis, e.g. card-index, list, register, file, record or a system containing files, documents, contracts, certificates, references, assessments, tests,
- h) purpose of personal data processing shall mean the aim of personal data processing that was previously explicitly specified or determined and is connected with certain activities,
- i) the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject knowingly signifies his agreement to personal data related to him being processed,
- j) transborder personal data flow shall mean transfer of personal data outside the territory of the Slovak Republic by an entity which has its registered seat or permanent residence abroad or their exchange with such entities,
- k) anonymous datum shall mean a personal datum adjusted in such manner that it cannot be matched with the concerned data subject,
- l) address shall mean a set of data concerning the residence of a natural person, including the name of the street, house number, registration number of house, name of municipality, if appropriate name of a municipality part, postal code, name of district, name of state,
- m) identifier of general application shall mean a permanent identification personal datum of the data subject securing its definiteness in filing systems,
- n) biometric datum shall mean personal datum of the natural person based on which the person is clearly and unequivocally identifiable, e.g. fingerprint, palm print, analysis of DNA, DNA profile,
- o) audit of the filing system security shall mean an independent expert evaluation of reliability and overall security of the filing system from the viewpoint of securing confidentiality, integrity and availability of the processed personal data,
- p) third country shall mean a country which is not a member of the European Union,
- r) public interest shall mean an important interest of the State pursued in the exercise of public authority, which overrides the legitimate interest of the natural person or several natural persons, brings financial or other benefit to other natural persons or to many of them and without pursuing of which an extensive or irrecoverable damages could be caused,
- s) conditions of the personal data processing shall mean the means and manner of the personal data processing, as well as other requirements, criteria or instructions concerning the personal data processing or the taking of the actions serving for achieving the purpose of the processing, whether prior to the personal data processing or in the course of their processing.

(2) Controller shall mean a state administration authority, territorial self-government authority, other public authority body or legal or natural person, which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of the processing of personal data are regulated by a special Act, the controller shall be the authority determined thereby for fulfilment of the purpose of the

processing or the authority, which fulfils the requirements stipulated by law. The same shall apply if so stipulated by the Directive of the European Communities and the European Union.

(3) Processor shall mean a state administration authority, territorial self-government authority, other public authority body or other legal or natural person processing personal data on behalf of the controller or controller's representative.

(4) Entitled person shall mean any natural person disposing of personal data within the framework of his employment relationship, civil service employment relationship, civil service relationship, membership, based on authorization, election or appointment or within the framework of performance of a public office, who may process personal data only upon instruction of the controller, controller's representative or processor, unless otherwise stipulated by this Act or by a special Act.

(5) Data subject shall mean any natural person whose personal data are processed.

(6) Controller's representative shall mean a legal or natural person representing the controller on the territory of the Slovak Republic, while the controller has his registered office or permanent residence in a third country.

(7) Third party shall mean a state administration authority, territorial self-government authority, other public authority body or any legal or natural person other than the data subject, controller or controller's representative, his processor and their entitled persons.

(8) Recipient shall mean a state administration authority, territorial self-government authority, other public authority body or other legal or natural person, to which the personal data were provided or made available; the controller authorized to process personal data under Section 2 Paragraph 1 Subparagraph f) and the Office fulfilling the tasks stipulated by this Act shall not be deemed a recipient.

P A R T T W O

RIGHTS, OBLIGATIONS AND RESPONSIBILITY IN THE PROCESSING OF PERSONAL DATA

C H A P T E R O N E

PRINCIPLES OF THE PROCESSING OF PERSONAL DATA

Section 5

Controller and Processor

(1) Personal data may be processed only by the controller or processor.

(2) Processor shall be entitled to process personal data only in the extent and under conditions agreed upon with the controller in a written contract or written authorization. The processor shall be entitled to process personal data only in the extent and under conditions agreed upon with the controller, or with another processor, provided that the controller gives consent to it in a written contract or written authorization.

(3) While selecting the processor the controller shall, in particular, mind his/her guarantees in the field of technological, organisational and personal safety measures (Section 15 paragraph 1). The controller may not entrust personal data processing to a processor if that could present a risk to the rights and law protected interests of data subjects.

(4) If the controller tasked the processor with the processing after acquiring personal data he should inform the data subjects of this fact during the next contact, however, not later than three months from the day of tasking the processor. This shall also apply when data processing is taken over by another controller.

(5) The controller's representative shall be obliged to act within the scope of the controller's rights and obligations stipulated by this Act. The provisions of this Act under which the Office imposes on the controller to do something, refrain from doing something or bear something, shall apply to the controller's representative accordingly.

Section 6

Basic Obligations of Controller

(1) The controller shall be obliged to

- a) determine unambiguously and concretely the purpose of the processing of personal data before starting the processing of personal data; the purpose of the processing of personal data must be clear and it cannot be contrary to the Constitution of the Slovak Republic, constitutional laws, laws and international treaties binding for the Slovak Republic,
- b) determine the means and manner of the processing of personal data, if appropriate other conditions of the processing of personal data,
- c) obtain personal data solely for a defined or determined purpose; obtaining of personal data under the pretext of a different purpose or activity shall be inadmissible,
- d) ensure that only such personal data are processed, the extent and contents of which correspond with the purpose of their processing and are necessary for its achieving,
- e) obtain personal data separately for various purposes and ensure that personal data are processed and used solely in the manner adequate to the purpose for which they were collected; combining of personal data obtained for various purposes shall be inadmissible,
- f) process only accurate, complete and, where necessary, updated personal data in respect of the purpose of their processing; the controller shall be obliged to block inaccurate and incomplete personal data and rectify or complete them without undue delay; inaccurate or incomplete that cannot be rectified or completed in order to make them accurate and complete shall be clearly marked by the controller and destroyed as soon as possible,
- g) ensure that the collected personal data are processed in the manner enabling identification of data subjects only during a time period necessary for achieving the purpose of processing,
- h) destroy the personal data whose purpose of processing terminated; personal data may be further processed also after termination of the purpose of the processing only under conditions stipulated in Paragraph 3,

i) process personal data in accordance with morality and act in a manner not contrary to, or circumventing, this Act or other generally binding legal regulations; neither the controller may force data subject's consent or make it conditional with a threat of rejecting the contractual relation, service, goods or duty of the controller or processor laid down by law.

(2) The controller shall be exempted from the obligation under Paragraph 1 Subparagraph a) only if the purpose of the processing of personal data is stipulated by a special Act in accordance with the conditions referred to in Paragraph 1 Subparagraph a). The controller shall be exempted from the obligation to determine the means and manner of the processing of personal data under Paragraph 1 Subparagraph b) only if they are stipulated by a generally binding legal regulation. The controller shall be obliged to fulfil the rest of the obligations under Paragraph 1 Subparagraphs c) to h) and i) of the part of the sentence before the semicolon also in the course of the processing of personal data pursuant to a special Act; this shall not affect the provision of Section 7 Paragraph 6 first sentence including its part after the semicolon.

(3) Further processing of the collected personal data for historical, scientific or statistical purposes shall not be deemed incompatible with the original purpose of the processing determined in accordance with Paragraph 1 Subparagraph a) or stipulated under Paragraph 2 first sentence. It is admissible to further process the collected personal data in the necessary extent for the historical, scientific or statistical purposes after termination of the original purpose of processing only provided that the controller

- a) guarantees that he would not use the processed personal data contrary to the legitimate interests of the data subject and by his conduct he would not infringe the right to protection of data subject's personal rights and privacy,
- b) duly denotes such personal data and make them anonymous as soon as possible or destroys them when they become useless.

(4) The controller who authorized the processor for processing of personal data shall be obliged to ensure that the processor fulfils the obligations under Paragraph 1 Subparagraphs c) to i) and Paragraph 3.

(5) In the case of doubts whether the extent, content and manner of processing or use of the processed personal data answer the purpose of their processing, whether they are compatible with the given purpose of processing or whether they are not up-to-date, as regards to the time and subject-matter, in respect to this purpose, the respective decision shall be made by the Office. The decision of the Office shall be binding.

Section 7

Consent of Data Subject

(1) Personal data may only be processed upon consent of the data subject, unless otherwise stipulated by this Act. This shall not affect the provisions of Paragraph 5 first sentence, Section 8 Paragraph 4 Subparagraph b), Section 9 Paragraph 1, Section 9 Paragraph 1 Subparagraphs b) and c), Section 10 Paragraph 6, Section 23 Paragraph 4 Subparagraph a) and Section 23 Paragraph 5.

(2) If the controller processes the personal data upon consent of the data subject, in the case of doubts he shall be obliged to prove to the Office, anytime upon its request, that he has

such consent at his disposal. The consent shall be proven by an audio or audio-visual recording or by an affidavit of the person that provided the personal data to the filing system, or by another reliable manner. The controller shall prove to the Office that he was given a written consent by a document proving obtaining of such consent. The evidence of such consent shall be constituted above all by information who gave the consent, to whom it was given, for what purpose, a list or extent of personal data, validity term of the consent and the terms of its cancellation. A written consent without own signature of the person who gave the consent shall be invalid.

(3) The consent under Paragraph 1 shall not be required if personal data are processed pursuant to a special Act⁴⁾ stipulating a list of personal data, the purpose of their processing and the group of data subjects. The processed personal data of the data subject may be provided, made available or made public in the filing system only if the special Act stipulates the purpose of provision, making available or public, a list of personal data that may be provided, made available or made public, as well as the third parties to which personal data are provided or a group of recipients to which personal data are made available, unless otherwise stipulated by this Act. This shall not affect the provision of Section 9 Paragraph 1 Subparagraph a).

(4) Personal data may be processed without consent under Paragraph 1 only if

- a) the processing of personal data is necessary for the purpose of artistic or literary expression, for the purpose of informing the public by means of the mass media and if the personal data are processed by a controller for whom it results from the scope of his activities; this shall not apply if by the processing of personal data for such purpose the controller violates the data subject's right to protection of his personal rights and privacy or if such processing of personal data without consent of the data subject is prohibited by a special Act or an international treaty binding for the Slovak Republic; or
- b) the processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to establish relations or take steps at the request of the data subject prior to entering into a contract; or
- c) processing of personal data is necessary for protection of life, health or property of the data subject or of another natural person without legal capacity or physically unable to give a consent and a consent of his legal representative cannot be obtained; or
- d) the subject of the processing is constituted solely by the title, name, surname and address of the data subject without a possibility of adding his other personal data and they are to be used solely for the controller's needs concerning the mail correspondence with the data subject and the keeping of records of such data; if the scope of the controller's activities is direct marketing, he may provide the above personal data, without a possibility of making them available and public only if they are to be provided to another controller whose scope of activities is also solely for the purposes of direct marketing and the data subject did not file an objection in writing under Section 20 Paragraph 3 Subparagraph c); or
- e) the processed personal data have already been made public; in such cases personal data must be duly denoted; or

⁴⁾ E.g. Sections 38 to 41 of the Act of the National Council of the Slovak Republic No. 387/1996 Coll. on Employment, Section 11a Paragraph 2 of the Act of the National Council of the Slovak Republic No. 542/1990 Coll. on State administration in Educational System and Educational Self-Administration, as amended by the Act No. 416/2001 Coll.

- f) processing of personal data is necessary for fulfilment of an important task carried out in the public interest; or
- g) processing of personal data is necessary for protection of statutory rights and legitimate interests of the controller or the third party, provided that in such processing of personal data the controller and the third party respect the fundamental rights and freedoms of the data subject and by their conduct they do not violate his right to protection of his personal rights and privacy.

(5) Personal data of the data subject may be obtained from another person and processed in the filing system only upon a prior written consent of the data subject. This shall not apply if by provision of the data subject's personal data to the filing system the other person protects his statutory rights or legitimate interests or notifies of the facts justifying enforcing of the data subject's legal liability or if personal data are processed pursuant to a special Act under Paragraph 3 or Section 9 Paragraph 1 Subparagraph a). The person processing personal data in this manner must be able to prove to the Office, anytime upon its requests, that he obtained them in accordance with this Act.

(6) A list of personal data under Paragraph 3 and Section 9 Paragraph 1 Subparagraph a) may be replaced by determining the extent of personal data only if individual personal data that are supposed to undergo the processing cannot be concretely determined with respect to the purpose of the personal data processing stipulated by a special Act; in such processing of personal data the controller shall be obliged to proceed pursuant to Section 6 Paragraph 1 Subparagraph d), with exception of those controllers who process personal data for the purpose of judicial proceedings and in connection with them. A list of third parties under Paragraph 3 and Section 9 Paragraph 1 Subparagraph a) may be replaced by determining a group of third parties only in the case that individual third parties to which personal data are to be provided cannot be specified in advance with respect to the nature of the matter, or if the third parties constitute a group of entities with the same scope of activities and if they process personal data for the same purpose or purposes, or if composition of such group is subject to a constant change.

(7) The person intending to make personal data of the data subject public cannot violate, by his conduct, the data subject's right to protection of personal rights and privacy; they cannot be made public contrary to legitimate interests of the data subject.⁷⁾

(8) If the data subject does not enjoy full legal capacity,⁸⁾ a consent required under this Act may be provided by his legal representative.⁹⁾

(9) If the data subject does not live, a consent required under this Act may be provided by his close person.¹⁰⁾ The consent shall not be valid if any close person expresses his disagreement in writing.

(10) The provision of Paragraph 6 shall also apply in the cases when provisions of Section 5 Paragraph 2 or Section 10 Paragraph 1 or 2 are followed.

⁷⁾ Sections 11 to 16 of the Civil Code.

⁸⁾ Section 8 of the Civil Code.

⁹⁾ Sections 26 to 30 of the Civil Code.

¹⁰⁾ Section 116 of the Civil Code.

(11) Personal data of the data subject may be provided from the filing system to another legal person, natural person, or an entity residing abroad only upon a written confirmation that a consent was obtained, provided that this Act requires such consent; the person providing personal data in such manner may replace the written confirmation of the obtained consent by a written declaration of the controller stating that data subjects gave their consent, provided that the controller is able to prove that the written consent of data subjects was given.

(12) Personal data under Paragraph 4 Subparagraph c) and under Section 9 Paragraph 1 Subparagraph b) may be processed without consent of the data subject only if and until the reasons, which prevented obtaining of the data subject's consent exist. If the reasons ceased to exist, the person processing the personal data shall provide the data subject's consent.

(13) The person alleging to process personal data which have already been made public shall prove to the Office, upon its request, that the processed personal data have already been made public.

(14) Recipients may process the personal data of the data subject which have already been made public only for their own needs within the framework of purely personal or household activities.

§ 8

Special Categories of Personal Data

(1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or movements, trade-union membership, and the processing of data concerning health or sex life shall be prohibited.

(2) In the processing of personal data, an identifier of general application stipulated by a special Act¹¹⁾ may be used for the purposes of identification of a natural person only provided that its use is necessary for achieving the given purpose of the processing. Processing of a different identifier revealing characteristics of the data subject, or releasing of an identifier of general application shall be prohibited.

(3) Processing of personal data relating to a breach of provisions of the criminal law, misdemeanours act or civil law, or relating to execution of final judgements or decisions, may only be performed by a person entitled to it by a special Act.¹²⁾

(4) Biometrical data may only be processed under conditions stipulated by a special Act, provided that

- a) it expressly results for the controller from the Act; or
- b) the data subject gave a written consent to the processing.

(5) Personal data relating to mental identity of a natural person or his mental capacity to work may only be processed by a psychologist or by a person entitled to it by a special Act.¹³⁾

¹¹⁾ Act of the National Council of the Slovak Republic No. 301/1995 Coll. on National Identification Number.

¹²⁾ E.g. Section 40 Paragraph 2 Subparagraph d) of the Act No. 153/2001 Coll., Section 52 of the Act of the National Council of the Slovak Republic No. 372/1990 Coll. on Misdemeanours, as amended, Act of the National Council of the Slovak Republic No. 171/1993 Coll., as amended.

Section 9
Exceptions from Restrictions
in Processing of Special Categories of Personal Data

(1) The prohibition relating to the processing of personal data under Section 8 Paragraph 1 shall not apply if the data subject gave a written consent to their processing, or if

- a) the processing is required by a special Act stipulating a list of personal data, the purpose of their processing and the group of data subjects; the processed personal data of the data subject may be provided, made available or made public from the filing system only if the special Act stipulates the purpose of provision, making available or public, a list of personal data that can be provided, made available or public, as well as the third parties to which personal data are provided or a group of recipients to which personal data are made available, unless otherwise stipulated by this Act; or
- b) the processing is necessary for protection of vital interests of the data subject or of another natural person without legal capacity or physically unable to give a consent and a consent of his legal representative cannot be obtained; or
- c) the processing is performed within the framework of legitimate activities by acivil society, foundation or non-profit organisation providing generally beneficial services, by a political party or movement, trade-union organisation, church or religious society acknowledged by the State, and such processing only concerns their members or the natural persons which are in a regular contact with them with respect to their objectives, the personal data serve solely for their internal needs and will not be provided to a third party without a written consent of the data subject; or
- d) the processing concerns the personal data which have already been made public by the data subject or which are necessary for exercising his legal claim; or
- e) the processing is performed for the purposes of providing medical care and effecting public health insurance, provided that these data are processed by a provider of the medical care, a health insurance company or the Office for Internal Supervision over Health Care; or
- f) the processing is performed within the framework of social insurance, social security of policemen and soldiers, for the purposes of provision of social relief or assistance in distress or if the processing is necessary for the purposes of fulfilment of obligations or exercising the legitimate rights of the controller responsible for the processing in the field of labour law and employment services, and if it results for the controller from a special Act.^{13a)}

¹³⁾ E.g. Section 2 of the Act of the National Council of the Slovak Republic No. 199/1994 Coll. on Psychological Activities and the Slovak Chamber of Psychologists, the Act of the National Council of the Slovak Republic No. 542/1990 Coll. on State Administration in Educational System and Educational Self-Administration, as amended.

^{13a)} Act No. 461/2003 Coll. on Social Insurance, as amended, Act No. 328/2002 Coll. on Social Security of Policemen and Soldiers and Changing and Amending of Some Acts, as amended, Act No. 195/1998 Coll. on Social Relief, as amended, Act No. 599/2003 Coll. on Assistance in Distress and Changing and Amending of Some Acts, as amended, Act No. 5/2004 Coll. on Employment Services and Changing and Amending of Some Acts, as amended.

(2) The written consent of the data subject given under Paragraph 1 shall be invalid if its provision is prohibited by a special Act.

(3) The provision of Section 8 Paragraph 4 shall not apply to the processing of biometrical data, except for analysis of DNA and the DNA profile of natural persons for the purposes of registration or identification in entering the sensitive, especially protected facilities, the premises with reserved access or in accessing technical appliances or devices with a high rate of risk and in the cases of solely internal needs of the controller.

Section 10

Obtaining Personal Data

(1) The controller who intends to obtain personal data from the data subject shall be obliged to inform the data subject, at the latest during obtaining of the data, and notify him in advance of the following without being requested

- a) the name and registered office or permanent residence of the controller; if on the territory of the Slovak Republic the controller's representative acts on behalf of the controller which has registered office or permanent residence in a third country, the controller's representative shall also notify the data subject of the name and registered office or permanent residence of the controller,
- b) the name and registered office and permanent residence of the processor, provided that the processor obtains personal data on behalf of the controller or the controller's representative; in such case the processor shall be obliged to notify the data subject in time of information under this Subparagraph,
- c) the purpose of the personal data processing; and
- d) additional information in the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data, in particular the right to be informed about conditions of the processing of his personal data
 1. identification of the entitled person obtaining personal data or proving his pertinence, by a reliable document, to the entity, on behalf of which it acts; the entitled person shall be obliged to satisfy such request of the data subject without undue delay,
 2. advice on voluntariness or obligation to provide the requested personal data; if the data subject may decide about provision of his personal data, the controller shall notify the data subject on what legal basis he intends to process the data subject's personal data; if the obligation of the data subject to provide his personal data arises from a special Act, the controller shall inform the data subject which act imposes this obligation on the data subject and he shall warn the data subject of the consequences of refusing to provide the personal data,
 3. third parties, provided that it is expected or clear that personal data will be provided to them,
 4. group of recipients, provided that it is expected or clear that personal data will be made available to them,
 5. form of making public, provided that personal data are to be made public,

6. third countries, provided that it is expected or clear that personal data will be transmitted to these countries,
7. advice on the existence of the data subject's rights.

(2) If the controller did not obtain the data subject's personal data directly from the data subject, he shall be obliged to notify the data subject, without undue delay but at the latest in the time before providing them for the first time to a third party (if such provision was expected already in obtaining of the personal data), of the information under Paragraph 1 Subparagraphs a) to c) and of additional information in the extent necessary for safeguarding the rights and legitimate interests of the data subject with regard to all circumstances of the processing of personal data, in particular the right to be informed about conditions of the processing of his personal data

- a) advice on the possibility to decide on processing of the obtained personal data,
- b) list of personal data,
- c) third parties, provided that it is expected or clear that personal data will be provided to them,
- d) group of recipients, provided that it is expected or clear that personal data will be made available to them,
- e) form of making public, provided that personal data are to be made public,
- f) third countries, provided that it is expected or clear that personal data will be transmitted to these countries,
- g) advice on the existence of the data subject's rights.

(3) The data subject does not have to be notified of the information under Paragraph 1, provided that with regard to all circumstances the controller is capable of proving to the Office, anytime upon its request, that in the time of obtaining the personal data all necessary information have already been known to the data subject. The data subject does not have to be notified of the information under Paragraph 2 if

- a) with regard to all circumstances the controller is capable of proving to the Office, anytime upon its request, that all necessary information have already been known to the data subject in the time of the decisive event,
- b) the processing of personal data is permitted by a special Act or by an international treaty binding for the Slovak Republic,
- c) the subject of the processing is constituted solely by the personal data that have already been made public, or
- d) the processed personal data are intended for the purposes of artistic or literary expression, or for the purposes of informing the public by means of the mass media under the conditions stipulated in Section 7 Paragraph 4 Subparagraph a) the part of the sentence before the semicolon, or for historical or scientific research and development, or for the purposes of the State's statistics, and if with regard to all circumstances the controller is capable of proving to the Office, anytime upon its request, that provision of such information is objectively impossible or would involve disproportionate costs and effort.

(4) The controller obtaining personal data for the purposes of identification of a natural person at his single entrance of the controller's premises shall be entitled to request his name,

surname, title and Identity Card number¹⁴⁾, or the number of an official identity card, or the number of a travel document,¹⁵⁾ citizenship and for proving, by a submitted document, that the provided personal data are true. If the natural person identifies himself according to a special Act,¹⁶⁾ the controller shall only be entitled to request for the registration number of his official identity card. In such cases, Paragraph 1 shall not apply.

(5) The controller or the processor obtaining, making available or providing personal data on the premises accessible to the public shall ensure their processing in secrecy.

(6) The personal data necessary for achieving the purpose of the processing may only be obtained by photocopying, scanning or other recording of official documents on an information carrier upon a written consent of the data subject or if a special Act expressly permits their obtaining without a consent of the data subject.¹⁷⁾ Neither the controller nor the processor may force data subject's consent or make it conditional with a threat of rejecting the contractual relation, service, goods or duty of the controller or processor laid down by law.

(7) The premises accessible to the public may be monitored by means of a video recording or audio recording only for the purposes of the public policy and security, disclosing criminal activities or interference with the State's security, provided that the premises are clearly marked as being monitored. Marking of the fact that the premises are being monitored is not required if it is not stipulated by a special Act. The recording may only be used for the purposes of criminal prosecution or proceedings concerning misdemeanours, unless otherwise stipulated by a special Act.

(8) The controller who obtained personal data under Section 7 Paragraph 4 Subparagraph d) without the data subject being aware of that or directly from the data subject, shall provide the data subject, in the course of their first contact, with the information under Paragraph 1, and if the personal data are processed for the purposes of direct marketing, he shall also notify the data subject of his right to object in writing to their provision and use in the mail correspondence.

(9) The controllers whose scope of activity is direct marketing shall keep a list of the provided personal data under Section 7 Paragraph 4 Subparagraph d) in the following extent: name, surname, title and address of the data subject, date of their provision or the date of effectiveness of the prohibition of their further provision under Section 13 Paragraph 6, and the name of the legal or natural person to whom the above personal data were provided. The legal and natural persons to whom the above personal data were provided shall keep a list in the same extent.

¹⁴⁾ Act of the National Council of the Slovak Republic No. 162/1993 Coll. on Identity Cards, as amended.

¹⁵⁾ Act No.381/1997 Coll. on Travel Documents.

¹⁶⁾ E.g. Section 8 of the Act of the National Council of the Slovak Republic No. 46/1993 Coll., Section 8 of the Act of the National Council of the Slovak Republic No. 198/1994 Coll., Section 14 Paragraph 1 Subparagraph a) of the Act of the National Council of the Slovak Republic No. 171/1993 Coll., as amended, Section 9 of the Act No. 124/1992 Coll.

¹⁷⁾ E.g. Section 15 Paragraph 3 of the Act No. 200/1998 Coll. on Civil Service of Customs Officer and Changing and Amending of Some Acts.

Section 11

Truthfulness of Personal Data

Only true personal data may be provided to a filing system. Liability for false personal data shall be born by the person who provided them to the filing system.

Section 12

Accuracy and Keeping Personal Data Up-To-Date

(1) The controller shall ensure accurate and up-to-date personal data. Personal data given in compliance with Section 11 shall be considered accurate.

(2) Personal data shall be deemed accurate, unless the contrary is proven.

Section 13

Destruction of personal data

(1) After the purpose of processing is fulfilled, the controller shall provide for destruction of personal data without undue delay.

(2) The controller shall provide destruction of personal data, except for the personal data under Section 7 Paragraph 4 Subparagraph d), without undue delay also in the case that

- a) the reasons which prevented obtaining of a consent of the data subject (Section 7 Paragraph 12) ceased to exist and the consent was not given; or
- b) the data subject filed an objection under Section 20 Paragraph 3 Subparagraph a); the controller shall further proceed pursuant to Paragraph 5.

(3) Paragraph 1 shall not apply if

- a) a special Act stipulates a time limit¹⁸⁾, which prevents destruction of personal data without undue delay; after expiration of the time limit prescribed by law the controller shall provide destruction of personal data without undue delay,
- b) personal data constitute a part of archive documents,¹⁹⁾
- c) the written, audiovisual, audio or other recording containing personal data was included in pre-archive care;²⁰⁾ no processing of personal data may be performed in the course of pre-archive care except for their storage, and they may only be used for the purposes of civil proceedings, criminal prosecution or administrative proceedings.

(4) Storage time limits for written, audiovisual, audio or other recordings containing personal data and included in the pre-archive care may be determined only for the time necessary for exercising the rights or obligations stipulated by law.²¹⁾

¹⁸⁾ E.g. Sections 31 and 32 of the Act No. 563/1991 Coll. on Book-Keeping, as amended by the Act No. 336/1999 Coll.

¹⁹⁾ Section 2 Paragraph 1 of the Act of the National Council of the Slovak Republic No. 149/1975 Coll. on Archives, as amended by the Act No. 571/1991 Coll.

²⁰⁾ Section 6 of the Act of the National Council of the Slovak Republic No. 149/1975 Coll., as amended by the Act No. 571/1991 Coll.

²¹⁾ E.g. Sections 101 to 110 of the Civil Code.

(5) If the data subject files an objection under Section 20 Paragraph 3 Subparagraph b), the controller shall terminate without undue delay the use of the personal data referred to in Section 7 Paragraph 4 Subparagraph d) in the mail correspondence.

(6) If the data subject files an objection under Section 20 Paragraph 3 Subparagraph c), the controller shall notify of it without undue delay and in writing every person to which he provided the personal data referred to in Section 7 Paragraph 4 Subparagraph d); a ban of further provision of the above personal data shall apply to the controller and to every person to whom the controller provided them from the day following after the day of delivery of the data subject's objection or of delivery of the controller's notification in writing.

(7) If the recording made pursuant to Section 10 Paragraph 7 is not used for the purposes of criminal proceedings or proceedings concerning misdemeanours, the person who made it shall destroy it at the latest within seven days from the day following after the day on which the recording was made, unless otherwise stipulated by a special Act.

(8) Repealed as of 1 May 2005

Section 14

Notification of Rectification or Destruction

(1) The controller shall notify the data subject and every person to whom he provided personal data of rectification or destruction of the personal data within 30 days from its execution.

(2) Notification may be abandoned, provided that the rights of the data subject are not violated by such abandonment of notification of rectification or destruction.

C H A P T E R T W O

SECURITY OF PERSONAL DATA

Section 15

Liability for Security of Personal Data

(1) The controller and the processor shall be responsible for security of personal data by protecting them against accidental or unlawful damage or destruction, accidental loss, alteration, unauthorized access and making available, as well as against any other unauthorized forms of processing. For this purpose he shall take due technical, organisational and personal measures adequate to the manner of processing, while he shall take into account above all

- a) the existing technical means,
- b) the extent of possible risk that could violate security or functionality of the filing system,
- c) confidentiality and importance of the processed personal data.

(2) The controller and the processor shall take the measures under Paragraph 1 in the form of a security project of the filing system (hereinafter the ‘Security Project’) and they shall provide its development if

- a) special categories of personal data under Section 8 are processed in the filing system and the filing system is interconnected with a publicly accessible computer network or it is operated in a computer network interconnected with a publicly accessible computer network,
- b) special categories of personal data under Section 8 are processed in the filing system; in such case the controller and the processor shall only document the taken technical, organisational and personal measures in the extent stipulated by Section 16 Paragraph 3 Subparagraph c) and Paragraph 6; or
- c) the filing system is used for safeguarding the public interest under Section 2 Paragraph 1; the provision of Section 16 shall not apply to development of the Security Project only provided that an obligation to elaborate a Security Project pursuant to a special Act^{21a)} simultaneously applies to the respective case.

(3) Upon request of the Office the controller and the processor shall prove the extent and contents of the taken technical, organisational and personal measures under Paragraph 1 or 2.

(4) If the subject of the inspection is constituted by the filing systems under Paragraph 2, the Office shall be entitled to request the controller or the processor for submittal of an evaluation report on the outcome of an audit of the filing system’s security (hereinafter the “evaluation report”), provided that there are serious doubts about its security or about practical implementation of the measures referred to in the Security Project. The controller or the processor shall submit the evaluation report, not older than two years, to the Office without undue delay, otherwise he shall provide performance of an audit of the filing system’s security at his own expense and submit an evaluation report within three months from the day of the obligation’s imposition.

(5) The audit of the filing system’s security may only be performed by an external, professionally qualified legal or natural person, who did not participate in development of the Security Project of the respective filing system and there are no doubts about its impartiality.

Section 16

Security Project

(1) The Security Project shall define the extent and manner of the technical, organisational and personal measures necessary for elimination and minimizing of the threats and risks affecting the filing system from the viewpoint of impairing its security, reliability and functionality.

(2) The Security Project shall be developed in accordance with the basic rules of filing system’s security, the issued security standards, legal regulations and international treaties binding for the Slovak Republic.

^{21a)} Act No. 215/2004 Coll.

(3) The Security Project shall include above all

- a) a security policy,
- b) analysis of the filing system's security,
- c) security directives.

(4) The security policy shall specify the basic security objectives that must be achieved for protection of the filing system against violation of its security and it shall contain above all

- a) specification of the basic security objectives and the minimum required security measures,
- b) specification of the technical, organisational and personal measures for ensuring protection of personal data in the filing system and the manner of their use,
- c) definition of the filing system's environment and its relation to the possible security violation,
- d) definition of the limits determining residual risks.

(5) Analysis of the filing system's security shall mean a detailed analysis of the state of the filing system's security containing above all

- a) qualitative risk analysis, within of which the threats affecting individual items of the filing system capable of violating its security or functionality are identified; the result of the qualitative risk analysis shall be a list of threats that could endanger confidentiality, integrity and availability of the processed personal data, while it shall also state the extent of the possible risk, proposals of the measures eliminating or minimizing the affect of the risk and a list of the remaining risks,
- b) use of security standards and determination of other methods and means of the protection of personal data; evaluation of conformity of the proposed security measures with the applied security standards, methods and means shall constitute a part of the analysis of the filing system's security.

(6) Security directives shall specify and apply the conclusions resulting from the Security Project to the concrete conditions of the operated filing system and they shall include above all

- a) description of the technical, organisational and personal measures defined in the Security Project and their use in concrete conditions,
- b) the scope of powers and description of the permitted activities of individual entitled persons, the manner of their identification and authentication in accessing the filing system,
- c) the scope of liability of entitled persons and of the personal data protection official (Section 19),
- d) the manner, form and periodicity of performance of the inspection activities focused on observation of the filing system's security,
- e) procedures during breakdowns, failures and other extraordinary situations including preventive measures for restricting the occurrence of extraordinary situations and possibilities of an effective restoration of the state before the breakdown.

Section 17

Advice

The controller or the processor shall be obliged to advise the entitled persons on the rights and obligations stipulated by this Act and on the liability for their breach. The controller or the processor shall advise on the above before giving the first instruction to the entitled person to perform any processing operation with the personal data. The entitled person shall confirm the advice by his signature; the controller or the processor shall make a written record of the advice.

Section 18

Obligation to Maintain Secrecy

(1) The controller and the processor shall be obliged to maintain secrecy about the personal data which they process. The obligation to maintain secrecy also applies after termination of the processing. The obligation to maintain secrecy shall not apply to them if pursuant to a special Act it is necessary for fulfilment of the tasks of the law enforcement agencies; this shall not affect provisions of special Acts.²²⁾

(2) The entitled person shall be obliged to maintain secrecy about the personal data which he comes across; he must not use them even for his personal needs and he must not make them public, provide them or make them available to anybody without consent of the controller.

(3) The obligation to maintain secrecy under Paragraph 2 shall also apply to other natural persons, who come across the personal data at the controller's or processor's place within the framework of their activities (e.g. maintenance and service of the technical means).

(4) The obligation to maintain secrecy under Paragraph 2 shall also apply after termination of the function of the entitled person or after termination of his employment relationship or similar labour relation, as well as the civil service employment relationship or the relation under Paragraph 3.

(5) Paragraphs 1 to 4 and the obligation to maintain secrecy imposed on controllers, processors and entitled persons pursuant to special regulations²³⁾ shall not apply in respect of the Office in the course of fulfilment of its tasks (Sections 38 to 44).

²²⁾ E.g. Section 40 of the Act of the National Council of the Slovak Republic No. 566/1992 Coll. on National Bank of Slovakia, as amended by the Act No. 149/2001 Coll.

²³⁾ E.g. Section 6 Paragraph 1 of the Act No. 150/2001 Coll. on Tax Authorities and on Changing and Amending of the Act No. 440/2000 Coll. on Reports of Financial Control, Section 14 of the Act No. 330/2000 Coll. on Security Exchange, Section 134 of the Act No. 566/2001 Coll. on Securities and Investment Services and on Changing and Amending of Some Acts (Securities Act), Sections 91 to 93 of the Act No. 483/2001 Coll. on Banks and on Changing and Amending of Some Acts, Section 24 of the Act No. 24/1991 Coll. on Insurance Business, as amended, Section 81 e) and Section 240 Paragraph 5 of the Act No. 311/2001 Coll. Labour Code, Section 53 Paragraph 1 Subparagraph e) of the Act No. 312/2001 Coll. on Civil Service and on Changing and Amending of Some Acts, Section 9 Paragraph 2 Subparagraph b) of the Act No. 313/2001 Coll. on Public Service, Section 8 of the Act No. 367/2000 Coll., Section 80 of the Act of the National Council of the Slovak Republic No. 171/1993 Coll., as amended, Section 15 Paragraphs 2 and 3 of the Act of the National Council of the Slovak Republic No. 38/1993 Coll. on Organisation of the Constitutional Court of the Slovak Republic, on Proceedings before It and on Status of Its Judges.

Section 19

Internal Supervision of Personal Data Protection

(1) The controller shall be responsible for internal supervision of protection of personal data processed pursuant to this Act.

(2) If the controller employs more than five persons, he shall authorize a personal data protection official or several personal data protection officials in writing for the internal supervision; these persons shall supervise observation of statutory provision in the processing of personal data.

(3) The controller shall provide a professional training of the personal data protection official or several personal data protection officials. The scope of the professional training shall correspond, above all, with the scope of this Act and the tasks arising from it, and with the scope of international treaties on protection of personal data²⁴⁾ promulgated in the manner stipulated by law. The Office may request the controller to provide evidence that the professional training took place.

(4) Before commencement of the processing of personal data in the filing system the personal data protection official shall assess whether any danger of violation of the rights and freedoms of data subjects arises from their processing. The personal data protection official shall notify the controller in writing without undue delay of any determination of violation of the rights and freedoms of data subjects before commencement of the processing or of determination of a breach of statutory provisions in the course of the processing of personal data; if after the notification the controller fails to rectify the situation without undue delay, the personal data protection official shall notify the Office of it.

(5) The controller who authorized the personal data protection official in writing for internal supervision of personal data protection shall be obliged to notify the Office of the above in writing without undue delay, but at the latest within 30 days from the day of the authorization of the personal data protection official by means of a registered letter. The controller shall notify the Office of the following data:

- a) name, registered office or permanent residence, corporate form and identification number of the controller or the controller's representative,
- b) title, name, surname and date of birth of the personal data protection official,
- c) position of the personal data protection official,
- d) date of effectiveness of the written authorization of the personal data protection official,
- e) controller's declaration stating that the personal data protection official fulfils the conditions stipulated in Paragraph 12.

(6) The controller shall notify the Office of authorization of one personal data protection official, even if he authorized several personal data protection officials for internal supervision of personal data protection. If the controller replaces the personal data protection

²⁴⁾ E.g. Convention on Protection of Individuals in Automatic Processing of Personal Data (Notification No. 49/2001 Coll.).

official, of whom he notified the Office, by another personal data protection official, he shall proceed pursuant to Paragraph 5.

(7) The personal data protection official shall provide

- a) the necessary cooperation with the Office in fulfilment of the tasks within his scope of power; anytime upon request the personal data protection official shall be obliged to submit to the Office his written authorization, written notifications issued for the controller pursuant to Paragraph 4, to show the extent of the knowledge acquired at the professional training,
- b) fulfilment of the obligations under Paragraph 4,
- c) internal supervision of fulfilment of the controller's basic obligations under Section 6,
- d) advice to the entitled persons under Section 17,
- e) disposal of the applications of data subjects under Sections 20 to 22,
- f) implementation of the technical, organisational and personal measures and he shall supervise their application in practice; if the controller is obliged to elaborate a Security Project in accordance with Section 16 or documents pursuant to Section 15 Paragraph 2 Subparagraph b), he shall provide their elaboration,
- g) internal supervision of the selection of the processor pursuant to Section 5 Paragraphs 3 and 4, drafting of a written contract or written authorization for the processor in accordance with Section 5 Paragraph 2 and he shall be liable for its contents; in the course of duration of the contractual relation or authorization he shall verify observation of the agreed conditions,
- h) internal supervision of the transborder personal data flow,
- i) submittal of filing systems for a special registration and announcement of alterations and deregistration of filing systems from the special registration; he shall keep records, in the extent stipulated by this Act under Sections 29 and 30, of the filing systems that are not subject to registration and he shall make it available to anybody who requests it in accordance with Section 32.

(8) A controller employing less than six persons may authorize a personal data protection official in writing for internal supervision of personal data protection; this person shall supervise observation of statutory provisions in the processing of personal data.

(9) A controller employing less than six persons, who did not authorize a personal data protection official in writing for internal supervision of personal data protection shall be obliged to submit for registration the filing systems which are subject to registration under Section 25 of this Act.

(10) The controller shall be obliged to enable the personal data protection official to execute internal supervision of personal data protection independently and to accept his legitimate proposals; notification of deficiencies or making of a request by the personal data protection official in connection with fulfilment of his obligations under Paragraph 7 must not become an instigation or a reason for the controller's action that could cause damage to the personal data protection official.

(11) The Office shall be entitled to impose an obligation on the controller to authorize a different personal data protection official in writing for internal supervision of personal data

protection, provided that it is proven that the personal data protection official, who had originally been authorized in writing, failed to fulfil or did not fulfil sufficiently the obligations under Paragraph 7, or assessed incorrectly or applied incorrectly in practice the rights and obligations imposed on the controller by this Act, or fails to fulfil the conditions stipulated in Paragraph 12. The controller shall be obliged to satisfy the request of the Office without undue delay and authorize a different person in writing for the internal supervision; if the above is prevented by the reasons worth special consideration that can be credibly proven by the controller to the Office, the Office shall determine a time limit for the controller until when he shall be obliged to replace the personal data protection official, eventually for submitting the filing systems for registration.

(12) Only a natural person enjoying full legal capacity who meets the precondition of integrity under Section 35 Paragraph 4 first sentence may perform the function of the personal data protection official; integrity shall be proven by submittal of an extract from the Criminal Register not older than three months and the controller shall be obliged to keep it during performance of the function of the personal data protection official. A natural person, who is a statutory authority of the controller and a natural person, who is entitled to act on behalf of the statutory authority of the controller cannot perform the function of the personal data protection official. The personal data protection official shall have a status of the entitled person of the controller.

CHAPTER THREE PROTECTION OF DATA SUBJECTS' RIGHTS

Section 20

Data Subject's Rights

(1) Upon a written application the data subject shall be entitled to request from the controller

- a) information about the state of processing of his personal data in the filing system in a generally intelligible form and in the extent under Section 26 Paragraph 3; if a decision under Paragraph 4 Subparagraph b) is issued, the data subject shall be entitled to familiarize himself with the procedure of the processing and evaluating of operations,
- b) exact information, in a generally intelligible form, about the source from which the controller obtained his personal data for their processing,
- c) a copy of his personal data, in a generally intelligible form, which constitute the subject of the processing,
- d) rectification of inaccurate, incomplete or not updated information, which constitute the subject of the processing,
- e) destruction of his personal data, provided that the purpose of their processing under Section 13 Paragraph 1 was fulfilled; if any official documents containing personal data constitute the subject of the processing, he may request their returning,
- f) destruction of his personal data, which constitute the subject of the processing, provided that the law was breached.

(2) The rights of the data subject may be restricted only under Paragraph 1 Subparagraphs d) and e), provided that such restriction results from a special Act or if exercising of this right would infringe the protection of the data subject or the rights and freedoms of others.

(3) The data subject shall be entitled to object to the controller, upon a free-of-charge written application, to the following

- a) processing of his personal data, in respect of which he expects that they are or would be processed for the purposes of direct marketing without his consent and he shall be entitled to request for their destruction,
- b) use of the personal data referred to in Section 7 Paragraph 4 Subparagraph d) for the purposes of direct marketing in the mail correspondence; or
- c) provision of personal data referred to in Section 7 Paragraph 4 Subparagraph d) for the purposes of direct marketing.

(4) The data subject shall be entitled to object to the controller anytime upon a free-of-charge written request or personally, provided that the matter cannot be postponed

a) to the processing of personal data in the cases under Section 7 Paragraph 4 Subparagraphs a), e), f) or g) by stating the legitimate reasons or by submitting evidence of infringement of his rights and legitimate interests that are or can be violated by the processing of personal data in a concrete case; if it is proved that the objection of the data subject is valid and the legitimate reasons do not prevent it, the controller shall be obliged to block the personal data, the processing of which was objected by the data subject without undue delay and destroy them as soon as possible,

b) and refuse to submit to the controller's decision, which would produce legal effects on him or significantly affect him, provided that such decision is based solely on the acts of the automatic processing of his personal data. The data subject shall be obliged to request the controller for examination of the issued decision by a method other than the automatic processing, while the controller shall be obliged to satisfy the request of the data subject in such manner that the entitled person shall have a decisive role in the examination of the decision; the controller shall inform the data subject about the manner of examination and the outcome of his finding in a time limit under Section 21 Paragraph 3. The data subject shall be deprived of the above right only if so stipulated by a special Act including measures for securing the legitimate rights of the data subject or if the above decision was made in the course of entering into, or performance of, a contract between the controller and the data subject, under condition that the request of the data subject contained in the contract was satisfied or that the data subject was granted the right, based on an agreement, to put his point of view anytime during the contract's validity.

(5) The data subject shall be entitled to disagree with the controller's decision under Section 23 Paragraph 5 and to refuse the transfer of his personal data to the third country, which does not ensure an adequate level of protection of personal data, provided that the transfer is to be made pursuant to Section 23 Paragraph 4 Subparagraph a).

(6) If the data subject suspects that his personal data are processed without authorization, he may notify the Office of it.

(7) If the data subject does not enjoy full legal capacity,⁸⁾ his rights may be exercised by his legal representative.⁹⁾

(8) If the data subject does not live, his rights arising from this Act may be exercised by his close person.¹⁰⁾

Section 21

Provision of Information to Data Subject

(1) The controller shall satisfy the requests of the data subject under Section 20 Paragraph 1 Subparagraphs a), d) to f) free of charge.

(2) The controller shall provide the information under Section 20 Paragraph 1 Subparagraphs b) and c) to the data subject free of charge, except for a fee in the amount not exceeding the amount of material costs accrued in connection with the making of copies, providing technical carriers and sending the information to the data subject, unless otherwise stipulated by a special Act.²⁶⁾

(3) The controller shall satisfy the requests of the data subject under Section 20 and notify him in writing at the latest within 30 days from the day of their receipt.

Section 22

Notification of Restriction of Data Subject's Rights

The controller shall notify in writing the data subject and the Office of restriction of the data subject's rights under Section 20 Paragraph 1 Subparagraphs d) and e) without undue delay.

C H A P T E R F O U R

TRANSBORDER PERSONAL DATA FLOW

Section 23

Transfer of Personal Data to Third Countries

(1) If the third country ensures an adequate level of protection of personal data, the personal data may be transferred to this country only under condition that the data subject was provided with the information under Section 10 Paragraph 1 or 2, or any of the conditions under Section 10 Paragraph 3 was fulfilled.

(2) The adequacy of the level of protection of personal data shall be assessed in the light of all the circumstances surrounding the transfer. Particular consideration shall be given to the respective legal regulations in the country of final destination with respect to the nature of the personal data, the purpose and duration of the processing.

²⁶⁾ E.g. the Act of the National Council of the Slovak Republic No. 162/1995 Coll., as amended.

(3) Personal data may be transferred to the third country, which does not ensure an adequate level of protection only based on a decision of the European Commission or if any of the conditions under Paragraph 4 is fulfilled.

(4) Where the country of final destination does not ensure an adequate level of protection, the transfer may be executed only under condition that

- a) the data subject gave a written consent to it, while knowing that the country of final destination does not ensure an adequate level of protection,
- b) it is necessary for performance of a contract between the data subject and the controller or for establishment of pre-contractual measures upon request of the data subject,
- c) it is necessary for entering into, or performance of, a contract concluded by the controller in the interest of the data subject with another entity,
- d) it is necessary for performance of an international treaty binding for the Slovak Republic or resulting from the laws due to an important public interest or for proving, filing or defending a legal claim,
- e) it is necessary for protection of vital interests of the data subject; or
- f) it concerns the personal data, which constitute a part of the lists, registers or files and are kept and publicly accessible pursuant to special Acts or are available, under these Acts, to the persons which prove a legal claim and fulfil the conditions prescribed by law for making them available.

(5) If the controller decides to transfer personal data to the third country, which does not ensure an adequate level of protection after their obtaining, he shall notify the data subject before the transfer of the personal data of the reason of his decision and advise the data subject about his right to refuse such transfer under Section 20 Paragraph 5, provided that the transfer is to be executed under the condition referred to in Paragraph 4 Subparagraph a); the controller shall be entitled to execute the proposed transfer of personal data only after obtaining a written consent of the data subject.

(6) If the controller authorizes an entity residing abroad for the processing of personal data on the controller's behalf, this entity shall be entitled to process the personal data only in the extent and under conditions agreed upon with the controller in a written contract. The scope of the contract must be elaborated in accordance with the standard contractual terms stipulated for the transfer of personal data by an entity residing abroad processing them on the controller's behalf.

(7) A consent of the Office shall be necessary for transfer of personal data under Paragraph 6.

(8) The person executing transfer of personal data shall ensure their security (Section 15 Paragraph 1) also during the transit.

(9) Protection of personal data transferred to the territory of the Slovak Republic from the entities with registered office or permanent residence abroad shall be executed in accordance with this Act.

(10) In the case of doubts whether a transborder personal data flow may be executed, a decision shall be made by the Office. The decision of the Office shall be binding.

Section 23a

Transfer of Personal Data within Member States of the European Union

(1) A free flow of personal data between the Slovak Republic and the Member States of the European Union shall be ensured; the Slovak Republic shall not restrict or prohibit transfer of personal data for the reasons of protection of fundamental rights and freedoms of natural persons, in particular their right to privacy in respect of processing of their personal data.

(2) The controller with the registered office or permanent residence on the territory of the Slovak Republic who simultaneously processes personal data by means of his organisational unit or several organisational units on the territory of one or several Member States of the European Union shall be obliged to take measures and ensure that each of his organisational units processes personal data in accordance with the laws in force in the Member State, where the respective organisational unit has its registered office.

(3) The controller, who does not have his registered office or permanent residence on the territory of a Member State of the European Union and for the purposes of processing of personal data he uses fully or partially automated or other than automated means of processing located on the territory of the Slovak Republic, while these means of processing are not used solely for the transfer of personal data through the territory of Member States of the European Union, shall be obliged to appoint, before commencement of the processing of personal data, his representative with the registered office or permanent residence on the territory of the Slovak Republic; this shall not affect the domestic law of the third country, in which the controller has his registered office or permanent residence. The controller's representative shall be obliged to prove to the Office anytime upon its request an original of the document confirming his appointment for the controller's representative. Authenticity of signatures and the print of the controller's stamp on the original document must be verified by the authority competent for its verification or by a notary in the respective State, while the verification must bear a stamp of the authority representing the Slovak Republic in this State.

CHAPTER FIVE

REGISTRATION AND RECORDS OF FILING SYSTEMS

Section 24

Obligation to Register and Keep Records

The controller shall register the filing systems or keeps records of them in the extent and under conditions stipulated by this Act.

R e g i s t r a t i o n

Section 25

Conditions of Registration

(1) The Office shall execute the registration of filing systems free of charge.

(2) The obligation to register shall apply to all filing systems, in which personal data are processed by fully or partially automated means of processing, except for the filing systems

- a) which are subject to a special registration under Section 27 Paragraph 2,
- b) which are subject to internal supervision of a personal data protection official, which was authorized by the controller in writing under Section 19 Paragraph 2 or 8 and executes internal supervision of personal data protection pursuant to this Act,
- c) containing personal data of natural persons processed for the purposes of fulfilment of pre-contractual relations or for the purposes of exercising the rights and obligations resulting for the controller from an existing or terminated employment relationship, civil service relationship, civil service employment relationship or membership relation with these natural persons, including personal data of their close persons,¹⁰⁾
- d) containing personal data concerning membership of the persons in a trade-union organisation, who are its members and if these personal data are processed by the trade-union organisation and used solely for its internal needs or containing personal data concerning religious beliefs of persons associated in a Church or religious association acknowledged by the State and if these personal data are processed by the Church or the religious association and used solely for their internal needs, or containing personal data concerning membership of persons in a political party or movement, of which they are members and if these personal data are processed by the political party or movement and used solely for their internal needs; or
- e) containing personal data necessary for exercising of the rights or fulfilment of the obligations arising from a special Act or which are processed pursuant to a special Act.

(3) Assignment of a registration number to the filing system and issuance of a confirmation of its registration shall constitute a part of the registration; if the condition under Section 26 Paragraph 2 is fulfilled, the processing of personal data in the filing system shall not be conditioned by an issuance of a confirmation of its registration.

(4) In the case of doubts whether the filing system is subject to registration, a decision shall be made by the Office. The decision of the Office shall be binding.

Section 26
Registration

(1) The controller shall be liable for submittal of his filing system for registration.

(2) The controller shall submit the filing system for registration before commencement of the processing of personal data.

(3) At submittal of the filing system for registration the controller shall state the following data:

- a) name, registered office or permanent residence, corporate form and identification number of the controller,
- b) name and surname of the statutory authority of the controller,
- c) name and surname of the personal data protection official performing internal supervision of personal data protection, provided that his appointment is required (Section 19 Paragraph 2),
- d) name, registered office or permanent residence, corporate form and identification number of the controller's representative, provided that he acts on the territory of the Slovak Republic on behalf of the controller, who has his registered office or permanent residence in a third country; in such case the data of the controller, who appointed the controller's representative shall be stated in Subparagraph a),
- e) name and surname of the statutory authority or member of the statutory authority of the controller's representative; in such case the data of the statutory authority or the member of the statutory authority of the controller, who appointed the controller's representative shall be stated in Subparagraph b),
- f) identifier of the filing system,
- g) purpose of the processing of personal data,
- h) list of personal data,
- i) group of data subjects,
- j) group of recipients, provided that it is expected or clear that the personal data will be made available to them,
- k) third parties or a group of third parties, provided that it is expected or clear that personal data will be provided to them,
- l) third countries, provided that it is expected or clear that personal data will be transferred to these countries and the legal basis of the transborder flow,
- m) legal basis of the filing system,
- n) the form of making public, provided that personal data are to be made public,
- o) general characteristics of the measures for ensuring protection of personal data,
- p) date of commencement of the processing of personal data.

(4) The data in the extent under Paragraph 3 shall be submitted to the Office in writing and they shall be confirmed by the controller's statutory authority or electronically in the form of a database file with an attached print copy of the contents of the file confirmed by the

controller's statutory authority. The written form and the format of the database file shall be determined by the Office. Attaching of the above copy shall not be required in the case that the database file bears an electronic signature pursuant to a special Act.

Section 27

Terms of Special Registration

- (1) The Office shall execute special registration of filing systems free of charge.
- (2) Special registration shall apply to the filing systems, in which the controller processes
 - a) at least one of the personal data referred to in Section 8 Paragraph 1, and at the same time their transfer to a third country or third countries not ensuring an adequate level of protection is expected or executed pursuant to Section 23 Paragraph 4 Subparagraphs a) or c),
 - b) personal data pursuant to Section 7 Paragraph 4 Subparagraph g); or
 - c) personal data pursuant to Section 9 Paragraph 3.
- (3) The controller shall be obliged to submit the filing system for the special registration at the Office before commencement of the processing of personal data.
- (4) In the case of the special registration the controller shall state the data in the extent under Section 26 Paragraph 3 and submit the base documents, which are necessary for the assessment of the processing in question. Section 26 Paragraph 4 shall apply accordingly to submittal of the filing system for the special registration.
- (5) The Office shall assess the submitted data under Paragraph 4, verify whether the processing of personal data could infringe the rights and freedoms of data subjects and decide, within 60 days from the day of their receipt, whether it will permit the processing of personal data; if the Office determines, during assessment of the submitted data, that the submitted filing system is not subject to a special registration, it shall notify the controller of it without undue delay.
- (6) In the case of doubts the Office shall request the controller for further explanations or base documents. The time limit under Paragraph 5 shall not pass during this time.
- (7) Assignment of a registration number to the filing system and issuance of a confirmation of its registration shall constitute a part of the special registration; the controller may commence the processing of personal data in the filing system submitted for a special registration on the day following after the day, when the Office issued the confirmation.
- (8) Provision of Section 28 shall apply to notification of alterations and deregistration of the filing system from the special registration.
- (9) If the Office assesses the processing of personal data in the filing system submitted for a special registration as a risk, it shall prohibit to the controller the processing of personal data for the respective purpose. The controller shall be obliged to respect the decision of the Office and to take measures, which will prevent the processing of personal data without undue delay.

Section 28

Notification of Alterations and Deregistration

(1) The controller shall notify the Office in writing of any alterations of the data under Section 26 Paragraph 3 except for Subparagraph p) which occurred in the course of the processing within 15 days.

(2) The controller shall deregister the filing system from the registration in writing within 15 days from the day of termination of the processing of personal data in the filing system. The date of termination of the processing of personal data shall constitute a part of deregistration.

(3) The provision of Section 26 Paragraph 4 shall apply accordingly to the notification of alterations of data and deregistration of the filing system.

R e c o r d s

Section 29

Terms of Records

(1) The controller shall keep records of the filing systems on his own, which are not subject to registration, at the latest from the day of commencement of the processing of personal data in these filing systems.

(2) Paragraph 1 shall not apply to the filing systems if

- a) the processed personal data serve solely for the needs of the mail correspondence with the data subjects and for keeping records of these data [Section 7 Paragraph 4 Subparagraph d)]; or
- b) they contain personal data processed solely for the purposes of identification of persons at their single entrance of the controller's premises (Section 10 Paragraph 4).

Section 30

Contents of Records

The records under Section 29 Paragraph 1 shall contain the data referred to in Section 26 Paragraph 3.

Making of the State of the Registration and Records Available

Section 31

Public Character of Registration

The registration executed pursuant to this Act shall be public in the extent of the data under Section 26 Paragraph 3, while the registration number of the filing system must be stated.

Section 32

Public Character of Records

The records kept pursuant to this Act shall be public. The controller shall make the data from the records available free of charge to anybody who requests it.

PART THREE

OFFICE

CHAPTER ONE **STATUS AND POWERS OF THE OFFICE**

§ 33

Scope of Powers of the Office

(1) An Office for Personal Data Protection of the Slovak Republic is hereby established and it shall constitute a state administration authority with competence over the entire territory of the Slovak Republic and the seat in Bratislava.

(2) The Office, as a state authority, shall execute supervision of personal data protection independently and it shall participate in protection of the fundamental rights and freedoms of natural persons in the processing of personal data.

(3) If personal data are processed by intelligence services, the supervision of personal data protection under Paragraph 2 shall be executed by the National Council of the Slovak Republic pursuant to a special Act.²⁷⁾

(4) The Office shall fulfil an obligation to notify the European Commission in the field of personal data protection.

(5) The Office shall take measures in order to execute the decisions of the European Commission issued in the field of the personal data protection.

²⁷⁾ Section 60 of the Act of the National Council of the Slovak Republic No. 350/1996 Coll. on Rules of Procedure of the National Council of the Slovak Republic.

(6) The Office shall cooperate in the execution of supervision of personal data protection with similar authorities executing supervision abroad.

Section 34

Status of Office

(1) The Office is a budgetary organisation.²⁸⁾ The Office shall submit a proposal of the budget as a part of the chapter of the Governmental Office of the Slovak Republic. Only the National Council of the Slovak Republic may decrease the approved budget of the Office in the course of a calendar year.

(2) Details concerning organisation of the Office shall be regulated by the rules of internal governance.

Section 35

President of Office

(1) The Office shall be headed by the President of the Office.

(2) The President of the Office shall be elected and recalled by the National Council of the Slovak Republic upon proposal of the Government of the Slovak Republic. The Government of the Slovak Republic shall submit its proposal for election of the President of the Office for a new electoral period to the National Council of the Slovak Republic at the latest 60 days before termination of the term of office of the acting President of the Office. The term of office of the President of the Office shall be five years and he may be elected for maximally two consecutive terms. The President of the Office shall remain in the function also after termination of the term of office until the National Council of the Slovak Republic elects another President of the Office for the new term of office.

(3) Only a citizen, who is eligible for a deputy of the National Council of the Slovak Republic, is irreproachable, has a university education, has professional experience in the field of information technology or law of at least 10 years and is at least 35-years old, may be elected the President of the Office.

(4) For the purposes of this Act, an irreproachable citizen shall be deemed a citizen, who was not sentenced, by a final decision, for a deliberate crime or who was not sentenced to imprisonment without suspension. Irreproachability shall be proven by an extract from the Criminal Register not older than three months.

(5) The President of the Office must not be a member of a political party or movement.

(6) Remuneration and other essentials concerning the President of the Office shall be determined by the Government of the Slovak Republic pursuant to a special regulation.²⁹⁾

²⁸⁾ Section 21 Paragraph 1 and Paragraph 4 Subparagraph a) of the Act of the National Council of the Slovak Republic No. 303/1995 Coll. on Budgetary Rules, as amended.

²⁹⁾ Act No. 312/2001 Coll.

(7) During performance of the function, the President of the Office must not undertake business or perform other earning activities, except for scientific, pedagogical, publication, literary or artistic activities and administration of his own property and of the property of his minor children.

(8) During performance of his function the President of the Office shall have the right to access to the official secrets pursuant to a special regulation.³⁰⁾

(9) In the course of the term of office, as well as after its termination the President of the Office shall be obliged to maintain secrecy about the facts concerning the contents of the personal data, about which he learned during performance of his function.

(10) The President of the Office may be exempted from the obligation to maintain secrecy in a concrete case by the National Council of the Slovak Republic.

(11) The President of the Office shall be liable for his activities to the National Council of the Slovak Republic.

(12) Performance of the function of the President of the Office shall terminate before expiration of the term of office by

- a) resignation from the function,
- b) loss of eligibility for a deputy of the National Council of the Slovak Republic,
- c) effectiveness of a decision by which he was sentenced for a deliberate crime or by which he was sentenced for a crime and in his case the court did not decide on suspension of imprisonment,
- d) performance of activities not compatible with performance of the function; or
- e) death.

(13) The National Council may recall the President of the Office if

- a) his health condition has not allowed him to fulfil the obligations arising from the function on a long-term basis, but at least for one year,
- b) he breached the obligation to maintain secrecy in respect of the facts concerning the contents of personal data, about which he learned in connection with performance of his function.

The President of the Office shall be recalled from the function on the day following after the day when he received a decision of the National Council of the Slovak Republic on recalling from the function.

³⁰⁾ Section 31 Paragraph 1 Subparagraph h) of the Act No. 241/2001 Coll.

Section 36

Vice-President of Office

(1) During the time of his absence, the President of the Office shall be represented by a Vice-President of the Office. Apart from the above, the Vice-President shall fulfil the tasks imposed on him by the President of the Office.

(2) The Vice-President of the Office shall be elected and recalled by the Government of the Slovak Republic upon proposal of the President of the Office.

(3) Provisions of Section 35 Paragraphs 3 to 5, 7, 9 and 12 shall apply accordingly to the performance of the function of Vice-President of the Office.

(4) The Vice-President may be exempted from the obligation to maintain secrecy in a concrete case by the President of the Office.

Section 37

Chief Inspector and Inspectors

(1) Activities of inspectors shall be managed by the chief inspector.

(2) Inspectors shall execute inspection activities and shall be competent to fulfil the tasks of the Office.

(3) Inspectors shall be appointed and recalled by the Government of the Slovak Republic upon proposal of the President of the Office. Only a citizen, who is eligible for a deputy of the National Council of the Slovak Republic, is irreproachable, has a university education, has professional experience in the field of information technology or law of at least three years and is at least 30-years old, may be elected the inspector of the Office. The chief inspector shall be appointed and recalled by the Government of the Slovak Republic upon proposal of the President of the Office out of the inspectors with a professional experience of at least five years and are at least 35-years old.

(4) The term of office of the chief inspector shall be five years and he can be appointed to the function repeatedly. Paragraphs 2 and 6 and provisions of Section 35 Paragraphs 4, 5, 7, 12 and 13 shall apply accordingly to performance of the function of the chief inspector.

(5) Provisions of Section 35 Paragraphs 4, 5, 7, 12 and 13 shall apply accordingly to performance of the function of the inspector. Apart from the reasons referred to in Section 35 Paragraph 13, the inspector can be recalled from the function due to

- a) a repeated failure to fulfil the tasks referred to in Section 38 Paragraph 1 Subparagraphs f) and h) or continuous minor breaches of work discipline, and if during the last six months the President of the Office repeatedly requested the inspector in writing to remove the defects and the inspector failed to remove them in a reasonable time; or

- b) gross neglect of an obligation imposed on the inspector by this Act [Section 38 Paragraph 1 Subparagraphs f) and h)], provided that he fails to prove that he did not cause the neglect or could not have prevented it, or due to a gross breach of the work discipline.

(6) In the course of duration of an employment relationship, as well as after its termination, inspectors and other employees of the Office shall be obliged to maintain secrecy in respect of the facts concerning the contents of personal data, about which they learned in connection with performance of their functions; the use of personal data in the fulfilment of the tasks of the Office or in connection with their fulfilment in accordance with the provisions of this Act or a special Act shall not be deemed a breach of the obligation to maintain secrecy. Inspectors and other employees of the Office may be exempted from the obligation to maintain secrecy in a concrete case by the President of the Office.

CHAPTER TWO ACTIVITIES OF OFFICE

Section 38

Tasks of Office

(1) The Office shall fulfil the following tasks during execution of supervision of personal data protection:

- a) inspect continuously the state of protection of personal data, registration of filing systems and keeping of records concerning the filing systems,
- b) recommend to controllers the measures for ensuring protection of personal data in the filing systems; for this purpose it shall issue recommendations for controllers within the scope of its power,
- c) in the case of doubts whether the extent, contents and the manner of processing and use of the processed personal data are adequate to the purpose of their processing, are compatible with the respective purpose of the processing or whether they are not up-to-date as regards to the time and subject-matter in respect of this purpose, it shall issue a binding decision,
- d) in the case of doubts about the transborder personal data flow, it shall issue a binding decision,
- e) in the case of doubts about registration of an filing system, it shall issue a binding decision,
- f) investigate notifications submitted pursuant to Section 45, or proceed upon an instigation or its own initiative pursuant to Section 44a and it shall issue measures for removal of defects,
- g) in the case of suspicion that the obligations imposed by this Act were breached it may call the controller or the processor and request them for an explanation,
- h) provide inspection of the processing of personal data in the filing systems,
- i) impose sanctions in the case of determining that the obligations referred to in this Act were breached,

- j) submit a notification³¹⁾ to the law enforcement agencies in the case of a suspicion that an offence was committed,
- k) execute registration of filing systems and provide access to the registration,
- l) participate in drafting of generally binding legal regulations in the field of personal data protection,
- m) issue generally binding legal regulations within the scope of its power,
- n) give opinions on draft laws and other generally binding legal regulations, which regulate processing of personal data,
- o) submit to the National Council of the Slovak Republic a report on the state of protection of personal data at least once in two years.

(2) Disputes arising from contractual or pre-contractual relations of controllers or processors and data subjects or other natural or legal persons, the hearing or deciding of which is subject to the respective courts or other authorities pursuant to special acts, shall not be the subject of the supervision of personal data protection.

(3) If the Office determines the facts indicating that an act, other generally binding legal regulation or an internal regulation issued by the controller violates the fundamental rights and freedoms of natural persons in the processing of their personal data, the President of the Office may file a petition with the respective authority for its amendment or cancellation.

I n s p e c t i o n A c t i v i t i e s

Section 39

Rights and Obligations of Inspection Authority

(1) The chief inspector and other inspectors (hereinafter the “inspection authority“), as well as the President of the Office and the Vice-President of the Office shall be entitled to

- a) enter the lands, buildings or premises of the operations and facilities of the controller and of the processor,
- b) request from the controller, processor and their employees (hereinafter the “inspected person”) to provide them in a determined time limit with documents and other papers, opinions and information, data processed on storage media including technical data carriers, reports and source codes of programs, provided that they own them, and other records necessary for execution of the inspection, originals or copies and to enable them, in justified cases, to make copies also outside the premises of the inspected person,
- c) request from the inspected person to provide, in a reasonable time limit, complete and true oral and written information, opinions and explanations in respect of the inspected and related facts and determined deficiencies,
- d) require cooperation of the inspected person,

³¹⁾ Section 158 Paragraph 1 of the Criminal Code.

- e) access the filing systems as the system administrator in the extent necessary for performing of the inspection,
- f) verify identity of the inspected persons and of the natural persons acting on behalf of the inspected persons.

(2) Inspection authority shall be obliged to

- a) notify the inspected person in advance of the subject-matter of the inspection and prove his relation to the Office before commencing the inspection,
- b) elaborate a protocol on execution of the inspection (hereinafter the “protocol”),
- c) state findings resulting from the inspection in the protocol,
- d) notify the inspected person of the findings resulting from the inspection and request him for a written opinion on all facts justifying enforcing of the legal liability; state in the protocol the objections filed to the findings resulting from the inspection from the viewpoint of their truthfulness, completeness and provability,
- e) give to the inspected person one copy of the protocol or of a record of the inspection or their copies,
- f) confirm to the inspected person in writing the receipt of the copies of documents, written documents, copies of storage media and of other records and ensure their due protection against loss, destruction or abuse.

(3) The protocol shall contain the name, registered office or permanent residence of the inspected person, place and time of the executed inspection, subject-matter of the inspection, name of the person who executed the inspection, the proved findings resulting from the inspection, opinions of the inspected person on the finding resulting from the inspection, date of elaboration of the protocol, names, official positions and own signatures of the inspection authority and the responsible employees of the inspected person who were notified of the contents of the protocol, and the date of their notification of the protocol. If the inspected person refuses to read the protocol, to give his opinion on the findings resulting from the inspection or to sign the protocol, this fact shall be stated in the protocol.

(4) If the inspection determines that the obligations stipulated by this Act were breached, the inspection authority shall proceed pursuant to Section 46 in the taking of measures for removal of deficiencies determined by the inspection.

(5) If the inspection does not determine any breach of the obligations stipulated by this Act or another Act³²⁾ the inspection authority shall only make a record of the inspection. Paragraph 3 shall apply accordingly to its elaboration.

Section 40

Rights and Obligations of the Inspected Person

(1) In the time of learning about the findings resulting from the inspection, the inspected person shall be entitled to file objections to the findings resulting from the inspection from the viewpoint of their truthfulness, completeness and provability.

³²⁾ E.g. Sections 178 and 257a of the Criminal Code.

- (2) The inspected person shall be obliged to
- a) create adequate conditions to the inspection authority for execution of the inspection and processing of the findings resulting from the inspection,
 - b) provide the inspection authority with the necessary cooperation in accordance with the rights under Section 39 Paragraph 1 and refrain from a conduct that could frustrate the execution of the inspection,
 - c) appear in a determined time at a place determined by the inspection authority in order to read the protocol,
 - d) sign the protocol or the record of the inspection after learning about the findings resulting from the inspection; the inspected person's refusal to read the protocol or to sign it shall not affect the consequences resulting from the contents of this document,
 - e) submit to the inspection authority in writing and in determined time limits the measures taken in order to remove the deficiencies determined by the inspection and a written report on fulfilment of these measures.

Section 41

Called Persons

(1) If justified by a special nature of the inspection task, the inspection authority may call other natural persons to execute the inspection. Participation of these natural persons in the inspection shall be deemed another action in a general interest. Provisions of Section 37 Paragraph 6 and Section 39 Paragraph 1 shall apply accordingly to the called persons.

(2) The inspection cannot be executed by the called persons who could raise doubts about their impartiality with regard to their relation to the subject-matter of the inspection or to the inspected person. The called persons who are themselves aware of the facts raising doubts about their impartiality shall notify the Office of these facts without undue delay.

(3) The inspected person may file provable objections to the bias of the called person in writing. Until a decision is made on the objections to bias, the called person may only take the actions not allowing postponing in the course of the inspection.

(4) Objections to bias and notification of bias shall be decided upon by the President of the Office. The decision of the President of the Office in this matter shall be deemed final.

Section 42

(1) Fulfilment of a concrete task within the execution of the inspection may also be imposed on other employees of the Office. Provisions of Section 39 Paragraph 1 and Paragraph 2 Subparagraph a) shall apply accordingly to the authorized employees of the Office.

(2) The inspectors and the authorized employees of the Office, who are themselves aware of the facts raising doubts about their impartiality with regard to their relation to the subject-matter of the inspection or to the inspected person shall notify the President of the Office of

these facts without undue delay. If the President of the Office considers the objection to bias justified, he shall exclude the person from acting in the matter.

Section 43

The regulations on the inspection in the State administration shall not apply to the execution of the inspection.³³⁾

C o o p e r a t i o n

Section 44

(1) State administration authorities, territorial self-government authorities, other state authority bodies, controllers and processors shall provide the Office with the necessary assistance in fulfilment of its tasks (Section 38).

(2) During fulfilment of the tasks of the Office the controller and the processor shall provide the Office with all requested data in a determined time limit.

(3) The controller and the processor shall appear at the Office upon its summons in a determined time limit in order to provide explanations.

(4) The controller and the processor shall be obliged to bear all actions taken by the Office with the aim to clarify the circumstances necessary for an objective assessment of an investigated case.

P r o c e e d i n g s

Section 44a

(1) Proceedings concerning the matters regulated by this Act, to which the general regulation on administrative proceedings does not apply, shall be initiated on the day when the Office took the first action against the controller, processor or other legal or natural person (hereinafter the “party to the proceedings”). If the proceedings are initiated upon petition of a party to the proceedings, the day of the petition’s delivery to the Office shall be deemed the day of initiation of the proceedings.

(2) A party to the proceedings shall be deemed the person whose rights or obligations are to be heard in the proceedings. A party to the proceedings other than a natural person shall be represented by a statutory authority or by its employee or member, who shall prove by a written authorization of the statutory authority that he is entitled to act on its behalf, unless otherwise stipulated by individual provisions of this Act. A party to the proceedings may be represented in the proceedings. A party to the proceedings may only have one representative for the same case, which it shall authorize in writing for the entire proceedings or only for certain acts. An authorization for representation of a party to the proceedings other than a natural person must be delegated by a person entitled to act on its behalf.

³³⁾ Act of the National Council of the Slovak Republic No. 10/1996 Coll. on Inspection in State administration.

(3) The proceedings shall not be public. This shall not affect the provision of Section 48.

(4) All means, by which the facts of the case can be determined and clarified, and which are in accordance with legal regulations, may be used in the taking of evidence. The evidence shall be constituted, above all, by the statements of the parties to the proceedings, witness testimonies, documents, expert opinions, or professional opinions, reports, statements and certificates of authorities or other legal or natural persons, information which was made public, inspections and findings resulting from the inspection. A copy in a printed, photographic, audio, audio-visual or other generally intelligible form may also be used as evidence instead of an original document or original recording, provided that it is carried on a commonly accessible data carrier.

(5) Instead of evidence, the Office may admit an affidavit of a natural person. The Office shall not admit the affidavit if it is prevented by a general interest or if it would breach equality between the parties to the proceedings. An expert opinion cannot be replaced by an affidavit. The natural person shall be obliged to state true data in the affidavit. The Office must warn the natural person of legal consequences of a false affidavit.

(6) The Office may appoint an expert or experts pursuant to a special regulation,^{33a)} provided that an expert opinion is necessary for professional assessment of the facts important for a decision in the case and it may impose on the appointed expert to elaborate a written expert opinion independently or to comment, in the expert opinion, on the questions asked by the Office. For this purpose, the Office shall make the necessary data from the file accessible to the appointed expert. In connection with elaboration of the expert opinion the Office may impose on a party to the proceedings to provide the appointed expert with all important information, to submit or make available all necessary documents, base documents or items or to enable access to the hardware and software of the filing system, to provide it with the necessary explanations or to take or bear some action, provided that it is necessary for elaboration of the expert opinion.

(7) The party to the proceedings shall be obliged to submit evidence, of which it has knowledge, in order to support its allegations. The Office shall decide which of the submitted pieces of evidence will be taken and it shall also take other pieces of evidence not submitted by the parties to the proceedings, provided that they are necessary for determination and clarification of the facts of the case. The facts that are generally known or that are known to the Office from its activities do not have to be proven.

(8) The Office shall evaluate the evidence at its own discretion, each piece individually and all pieces in their mutual connection; at that, it shall take into account everything that was disclosed in the proceedings.

(9) Important documents, above all orders and decisions, shall be delivered to the party to the proceedings, addressee, or to the person, who identifies himself with an authorization for receiving mail, as a registered mail with an advice of delivery and a note "personal delivery". The documents for a party to the proceedings other than a natural person, shall be delivered to the persons or members entitled to receive documents on behalf of this entity or to the person

^{33a)} Act No. 382/2004 Coll. on Experts, Interpreters and Translators and on Changing and Amending of Some Acts.

entitled to act on behalf of this entity. The documents for the counsel may also be delivered to law clerks and other employees who work in the office of the counsel and are authorized by the counsel for receiving mail.

(10) If the addressee of the mail that was supposed to be delivered into his hands was not reached although he lives at the place of delivery, the postman shall notify him in a due manner that he would deliver the mail again on a determined day and time. If the new attempt to deliver the mail is vain, the postman shall deposit the mail at the post office and notify the addressee of it in a due manner. If the addressee fails to collect the mail within three days from its depositing, the last day of this time limit shall be deemed the day of delivery, even if the addressee did not learn about depositing of the mail.

(11) If the addressee orders delivering of mail to a P.O.BOX, the post office shall notify the addressee of arrival of the mail, of the times when it can be taken over and of the time limit for the takeover on a standard form, which it shall put in the P.O.BOX. If based on an agreement the addressee takes his mail over at the post-office and does not have a P.O.BOX, the post-office shall not notify of such mail. In both cases the day of arrival of the mail shall be deemed the day of depositing. If the addressee fails to collect the mail within three days of its depositing, the last day of this time limit shall be deemed the day of delivery, even if the addressee did not learn about depositing of the mail.

(12) A party to the proceedings which lives abroad or has its registered office or permanent residence abroad shall be obliged to designate, for delivery of mail, its representative with registered office or permanent residence on the territory of the Slovak Republic and it shall notify the Office in time of his name, surname and address.

(13) A document shall be deemed delivered upon its receipt by the party to the proceedings or upon return of the registered mail by the post-office as undeliverable or if delivery of the mail was frustrated by the conduct or negligence of the party to the proceedings. If the addressee refused to take the mail over groundlessly, the document shall be deemed delivered on the day when its receipt was refused; the postman must warn the addressee of this.

(14) If necessary, the Office shall determine a time limit for taking of an action in the proceedings, unless it is stipulated by this Act. This time limit shall not include the day, when the event determining the commencement of the time limit occurred. The time limits determined by weeks, months or years shall terminate upon expiry of the day, which corresponds with the day, when the event determining the commencement of the time limit occurred, and if such day does not exist in the respective month, the time limit shall expire on the last day of the month. If the last day of the time limit falls on Saturday, Sunday or a holiday, the nearest working day shall be deemed the last day of the time limit. The time limit shall be observed if on the last day of the time limit the document is submitted to the Office or to the post-office. In the case of doubts, the time limit shall be deemed observed, unless contrary is proven.

(15) The costs accrued to the party to the proceedings in the proceedings shall be born by the party to the proceedings. The costs accrued to the Office shall be born by the Office.

(16) The proceedings initiated upon the own initiative of the Office may be stayed if the reason for the proceedings ceased to exist or if it was proved, in the course of the proceedings, that the reasons for its continuation are not sufficient or if a party to the proceedings dies.

Section 44b

A party to the proceedings in the proceedings concerning imposition of a sanction for a breach of this Act pursuant to Section 49 or Section 50 shall be the controller, processor or a natural person, on whom a fine shall be imposed pursuant to this Act; the proceedings concerning imposition of the sanction for a breach of this Act shall be initiated by the Office upon its own initiative pursuant to a generally binding regulation on administrative proceedings and only for the purposes of imposition of the fine. The Office may issue a decision on imposition of the fine without further taking of evidence and determination of base documents for the decision,^{33b)} provided that based on the proven findings resulting from the inspection or the evidence taken in the course of the proceedings justifying enforcing of the legal liability of the party to the proceedings under this Act, the Office considers sufficiently determined and proven that provisions of this Act were breached, or based on determination of a breach of the provision of Section 40 Paragraph 2 Subparagraph a) or b) by the inspected person.

CHAPTER THREE RECTIFICATION MEASURES

Section 45

Investigation of Notification

(1) In the execution of supervision of personal data protection the Office shall also use notifications and petitions of legal and natural persons (hereinafter the “notification“) concerning suspicion of a breach of the obligations or conditions stipulated by this Act. The notification shall be submitted to the Office in writing.

(2) Apart from the data subject, the notification may be filed under Section 20 Paragraph 6 also by a natural person alleging that his rights stipulated by this Act were directly infringed (hereinafter the “informant”).

(3) The Office shall file the notification away if

- a) the matter concerned by the notification is not within its competence,
- b) the particulars referred to in Section 9 were not completed or specified upon request of the Office in a determined time limit,

^{33b)} Sections 32 to 40 of the Act No. 71/1967 Coll. on Administrative Proceedings (Administrative Procedure Code), as amended by the Act. 527/2003 Coll.

- c) the informant fails to provide the Office with the necessary cooperation, upon request of the Office, while the matter cannot be disposed of without his active participation,
- d) the informant insists on maintaining his identity in secrecy in spite of the fact that the matter cannot be disposed of without using his personal data or some of his data under Paragraph 9 Subparagraph a),
- e) the informant files a repeated notification after expiration of the time limit under Paragraph 14.

(4) The Office may file the notification away, provided that it determines that

- a) the case concerned by the notification is heard by a court or other law enforcement agency,
- b) on the day of delivery of the notification more than three years elapsed from the taking of the measure or from the event concerned by the notification,
- c) the notification is manifestly unfounded,
- d) it does not contain the name, surname, address of the permanent residence and signature of the informant; such notification shall be deemed anonymous,
- e) notification informs about the case that has already been disposed of by the Office and the repeated notification does not contain any new acts.

(5) The Office shall inform the person who filed the notification that the notification was filed away and about the reasons for filing it away; this shall not apply in the case of an anonymous notification. The notification which was filed away shall be deemed disposed of.

(6) The notification shall not be admissible, if prior to its filing the informant failed to exercise his right under Section 20 provided by this Act. The Office shall file away the notification and notify the informant of a possibility to exercise his rights under Section 20.

(7) If the condition under Paragraph 6 was not fulfilled, the Office shall not file away the notification only in the case that the informant credibly proves that he did not fulfil this condition for the reasons worth special consideration.

(8) Investigation shall be deemed initiated on the day of delivery of a written notification to the Office. The Office shall notify the informant of the receipt of the notification, provided that the notification was not filed personally.

(9) The notification must contain above all

- a) the name, surname, address of the permanent residence and signature of the informant,
- b) identification of the person against whom the notification is filed; name or name and surname, registered office or permanent residence, or corporate form and identification number,
- c) the subject of notification stating which rights were violated by the processing of personal data according to the informant,
- d) evidence supporting the allegations stated in the notification,
- e) a copy of a document proving that the right under Section 20 was exercised, provided that such right could have been exercised or the reasons worth special consideration.

(10) If the notification fails to contain the particulars under Section 9, is not intelligible, or if data not stated in the notification are necessary for its due disposal, the Office shall request the informant to remove these defects in a determined time limit not shorter than seven days. At the same time it shall warn the informant of the consequences of a failure to remove the defects on the further course of the investigation. The time limit under Paragraph 12 shall not lapse during the time when the informant is in delay with fulfilment of this obligation.

(11) If the notification under Paragraph 9 does not contain the informant's request for maintaining his identity in secrecy, the Office shall dispose of the notification without maintaining the personal data referred to in Paragraph 9 Subparagraph a) in secrecy. If in the notification under Paragraph 9 the informant requests the Office for maintaining his identity in secrecy but the nature of the notification does not enable its investigation without stating some of the data of the informant, after determination of this fact the Office shall notify the informant of it. At the same time it shall notify the informant that disposal of the notification will continue only in the case that he gives, in a determined time limit, a written consent to the Office to state the necessary personal datum or data within the framework of the investigation.

(12) The Office shall investigate and dispose of the informant's written notification in a time limit of 60 days from the day of its receipt. In justified cases, the chief inspector may reasonably prolong this time limit, but not by more than six months. The Office shall notify the informant in writing of the prolonging of the time limit.

(13) In a time limit under Paragraph 12 the Office shall notify the informant in writing of the outcome of the notification's investigation, in which it shall state the informant's rights under this Act which were violated. If the Office does not determine any violation of the informant's rights, it shall notify him in writing about this fact without undue delay, but at the latest in a time limit under Paragraph 12. The notification shall be deemed disposed of by delivery of written information about the outcome of the notification's investigation to the informant.

(14) Notification concerning the same case may be repeated in a time limit of 30 days from the day of delivery of the outcome of the notification's investigation; if the notification does not contain new facts, the Office shall proceed pursuant to Paragraph 4 Subparagraph e). If the Office does not file the repeated notification away or if it finds out that it contains new facts, the chief inspector shall examine whether the original notification was disposed of duly; it shall notify the informant of the outcome in writing, while it shall proceed accordingly under 13. Examination of the notification by the chief inspector shall be deemed final.

(15) If the informant files a notification in the same case as has already been filed by another informant and disposed of, and if the notification does not contain any new facts, it does not have to be investigated again. However, the informant must be notified of the outcome of disposal of the original notification without undue delay, but at the latest in a time limit under Paragraph 12, first sentence.

(16) Filing of a notification must not be to the informant's detriment; this shall not apply if by the contents of his notification the informant commits a crime or misdemeanour.

(17) A notification filed by a legal or natural person other than the informant shall be disposed of like the proceedings initiated upon the own initiative of the Office, provided that it is proven, after examination of the notification, that there is a reason for initiating an investigation. Upon request of the legal or natural person which filed the notification with the Office, the Office shall confirm the receipt of the notification; the Office shall not notify it of the outcome of the investigation. The legal or natural person which filed the notification shall not be deemed a party to the proceedings.

Section 46

Order

(1) The Office

- a) before commencement of the processing of personal data or in the course of the processing of personal data it may impose on the controller or processor, in the extent necessary for achieving the purpose of the proceedings, to take, refrain or bear some action by an interim measures; in the case of suspicion that an obligation imposed by this Act was breached it shall request the controller or the processor for an immediate blocking of the personal data or for atemporary suspension of the activity that could endanger fulfilment of such obligation,
- b) if it determines that the controller or the processor failed to fulfil or breached any of the obligations stipulated by this Act, circumvented the provisions of this Act in the course of his fulfilment of any of the obligations, failed to observe or circumvented the conditions stipulated by this Act or processes or processed personal data contrary to this Act, it shall be obliged to impose on the controller or the processor to take measures, in a determined time limit, in order to remove the determined defects and causes of their origination. The Office shall be further entitled to take the following actions in respect of the controller or the processor
 1. impose an obligation to provide, in a determined time limit, elaboration or completing of documents or the Security Project in accordance with this Act,
 2. impose an obligation to take, in a determined time limit, the technical, organisational and personal measures adequate to the manner of the processing,
 3. prohibit processing of the personal data, the processing of which is contrary to the provisions of this Act,
 4. prohibit processing, which is contrary to the provisions of this Act,
 5. order removal or destruction of personal data in a determined time limit, provided that they are or were processed illegitimately; and
 6. impose on the controller an obligation to cancel, in a determined time limit, a written authorization or written contract with the processor.

(2) The controller and the processor shall satisfy the requests of the Office under Paragraph 1 without undue delay and inform the Office about their fulfilment in a determined time limit.

(3) The controller and the processor shall be entitled to file objections in writing to an order imposed under Paragraph 1 Subparagraph a) within three days from the day of its delivery. Objections to such order shall not have a suspensory effect.

(4) The controller and the processor shall be entitled to file objections in writing to a order imposed under Paragraph 1 Subparagraph b) within seven days from the day of its delivery. Objections to such order shall have a suspensory effect.

(5) The President of the Office shall decide on an objection of the controller or processor filed under Paragraph 3 within 15 days and he shall decide on an objection filed under Paragraph 4 within 60 days from the day of its receipt.

(6) The decision of the President of the Office on the objections shall be deemed final.

(7) The written appeal on taking of an order and the written decision on objections shall be delivered into the addressee's own hands.

(8) The Office may cancel an order imposed under Paragraph 1 Subparagraph a); its effectiveness shall terminate on the day of notifying of the measure under Paragraph 1 Subparagraph b) in the case in question.

Section 47

Provisions of Sections 45 and 46 shall not affect the right to a judicial protection.³⁵⁾

Section 48

Making of the Act Violation Public

(1) If the Office determines that the obligations stipulated by this Act were breached or that the provisions of this Act or of a special Act³²⁾ were circumvented, the President of the Office or the chief inspector may make public the business name or name, registered office or permanent residence, identification number, if assigned, and the corporate form of the person, who committed the illegal action and

- a) the verdict of an enforceable order and the grounds of the order or their parts under Section 46, except for personal data, if any are contained,
- b) the verdict of an enforceable decision and the grounds of the decision or their parts under Section 49 or Section 50, except for personal data, if any are contained; or
- c) characteristics of the facts of the case concerning the breach of protection of personal data.

(2) The President of the Office or the chief inspector may impose on the controller or the processor an obligation to make public the facts in the extent under Paragraph 1 Subparagraph c) in the mass media.

(3) The controller shall be obliged to fulfil an obligation imposed by the President of the Office or by the chief inspector under Paragraph 2. The statutory authority of the controller

³⁵⁾ Section 247 et seq. of Chapter Two of the Civil Procedure Code.

shall be obliged to provide making of a notice in the extent under Paragraph 1 Subparagraph c) public in the mass media at the expense of the controller; the contents, form, the mass medium and the latest possible day of making the notice public shall be determined by the President of the Office or by the chief inspector.

(4) An obligation under Paragraph 3 shall also apply to the processor.

CHAPTER FOUR SANCTIONS FOR THE ACT VIOLATION

Section 49

Administrative Offences

(1) The Office may impose a fine in the amount from SKK 50,000 to SKK 10,000,000 to the controller or the processor who

- a) failed to fulfil or breached any of the obligations stipulated in Sections 5, 6, 7, 10, or circumvented the provisions of this Act in the course of his fulfilment of any of the obligations stipulated in Sections 5, 6, 7, 10, or processes or processed personal data contrary to Sections 5, 6, 7, 10,
- b) failed to fulfil or breached any of the obligations stipulated in Sections 8, 9, or processes or processed special categories of personal data contrary to Sections 8, 9; or
- c) failed to take due technical, organisational and personal measures adequate to the manner of the processing or failed to prove, or could not prove, to the Office, upon its request, application of the measures in the practice pursuant to Section 15 Paragraphs 1, 3, or failed to take due technical, organisational or personal measures adequate to the manner of the processing in the form of a Security Project, or failed to submit to the Office, upon its request, a Security Project, while he was obliged to provide its elaboration under Section 15 Paragraphs 2, 3, or submitted a Security Project, which failed to contain the particulars stipulated by this Act under Section 16, or failed to submit to the Office, upon its request, the technical, organisational and personal measures adequate to the manner of the processing supported with documents, or failed to support with documents the technical, organisational and personal measures in the extent stipulated by this Act, while it was obliged to elaborate such documents under Section 15 Paragraph 2 Subparagraph b), or provably neglected the application, or failed to apply, in practice the technical, organisational and personal measures adequate to the manner of the processing referred to in the Security Project or in the documents under Section 15 Paragraph 2 Subparagraph b).

(2) The Office may impose a fine in the amount from SKK 50,000 to SKK 5,000,000 to the controller or the processor who

- a) failed to fulfil or breached any of the obligations stipulated in Section 13, or processes or processed personal data contrary to Section 13,
- b) failed to provide, upon request of the Office, execution of an audit of the filing system's security or provided execution of the audit of the filing system's security contrary to this

Act, or failed to submit in time an evaluation report under Section 15 Paragraphs 4, 5, or submitted an evaluation report not specifying the determined defects,

- c) failed to advise his entitled persons in time or could not credibly prove to the Office that he advised his entitled persons in time, or failed to submit to the Office, upon its request, a written record of advice of the entitled persons under Section 17; or
- d) transferred personal data to third countries contrary to Section 23, or processes or processed personal data contrary to any of the conditions stipulated in Section 23, Section 23a Paragraphs 2, 3, or failed to fulfil any of the obligations stipulated in Section 23, Section 23a Paragraphs 2, 3.

(3) The Office may impose a fine in the amount from SKK 30,000 to 3,000,000 to the controller who

- a) failed to fulfil the obligation of special registration of the filing system under Section 27, or failed to fulfil any of the obligations connected with the special registration arising from this Act under Section 28,
- b) failed to fulfil the obligation of registration of the filing system under this Act or failed to fulfil any of the obligations connected with registration of the filing system under Section 28,
- c) failed to authorize a personal data protection official in writing for execution of internal supervision of personal data protection or cannot credibly prove his authorization in writing under Section 19 Paragraph 2, or failed to provide professional training of the personal data protection official in accordance with this Act under Section 19 Paragraph 3; or
- d) provably failed to enable, disturbed, frustrated or otherwise obstructed to the personal data protection official fulfilment of his obligations stipulated by this Act, or failed to respect the legitimate written notifications of the personal data protection official under Section 19 Paragraphs 4, 7, 10.

(4) The Office may impose a fine in the amount from SKK 10,000 to SKK 1,000,000 to the controller who

- a) failed to fulfil the obligation to notify of rectification or destruction of personal data under Section 14,
- b) authorized in writing a natural person not fulfilling any of the conditions stipulated by Section 19 Paragraph 12 for acting as the personal data protection official, or cannot prove by an extract from the Criminal Register the irreproachability of the personal data protection official, or failed to fulfil or breached any of the obligations stipulated in Section 19 Paragraphs 5, 6, or failed to fulfil an obligation imposed by the Office under Section 19 Paragraph 11,
- c) failed to satisfy legitimate requests of the data subject, or failed to proceed in accordance with this Act in their disposal, or failed to provide the data subject with information in a time limit stipulated by law, or failed to inform the data subject in the manner stipulated by this Act under Section 20, 21,
- d) failed to notify of restriction of data subject's rights under Section 22; or
- e) failed to fulfil the obligation to keep records of the filing system under Sections 29, 30, or refused to make the data from the records available under Section 32.

- (5) The Office may impose a fine up to the amount of SKK 100,000 to the person who
- a) provides personal data contrary to Section 7 Paragraph 5; this shall not apply to the controller and the processor,
 - b) provides false personal data (Section 11),
 - c) breaches the obligation to maintain secrecy about personal data (Section 18); or
 - d) as a personal data protection official, fails to notify the controller in writing (Section 19 Paragraph 4).

(6) The Office may impose a fine under Paragraphs 1 to 4 and under Section 50 repeatedly, provided that the obligation was not fulfilled in a determined time limit.

(7) In the imposition of fines, the gravity, time of duration and consequences of the illegal conduct shall be taken into account above all.

(8) A fine under Paragraphs 1 to 5 may be imposed within one year from the day when the Office determined the breach of the obligation, but at the latest within three years from the day when the obligation was breached.

(9) In a decision on imposition of a fine, the Office may simultaneously impose on the obliged person to take measures in order to redress, in a determined time limit, the consequences of the illegal conduct.

(10) A remonstrance may be filed against the decision on imposition of a fine within 15 days from the day of its delivery. The President of the Office shall decide on the remonstrance within 60 days from the day of its receipt.

(11) Proceeds from the fines shall constitute an income of the State budget.

Section 50

Disciplinary Fines

- (1) The Office may impose a disciplinary fine to the controller or to the processor
- a) up to the amount of SKK 50,000, provided that he fails to provide adequate conditions for execution of the inspection [Section 40 Paragraph 2 Subparagraph a)],
 - b) up to the amount of SKK 500,000, provided that he frustrates execution of the inspection [Section 40 Paragraph 2 Subparagraph b)]; if the controller or the processor proves that frustration of execution of the inspection was caused by the entitled person, his liability shall be restricted and the entitled person shall also become liable,
 - c) up to the amount of SKK 1,000,000, provided that he failed to make public at all, or failed to make public in time, a notice designated to be made public in the mass media by the President of the Office or the chief inspector, or provided that he failed to make the above notice public in the determined form or in the determined mass medium, or provided that he failed to adhere to the determined contents of this notice under Section 48 Paragraphs 3, 4; the fine may be imposed repeatedly until fulfilment of the obligation,

- d) up to the amount of SKK 2,000,000, provided that he failed to provide the Office with the cooperation under Section 44 Paragraphs 2, 3, 4, or failed to satisfy the requests of the Office or failed to notify the Office in a determined time limit under Section 46 Paragraphs 1, 2.

(2) Disciplinary fine may be imposed within one year from the day when the obligation was breached.

P A R T F O U R

COMMON, INTERIM AND FINAL PROVISIONS

Section 51

Common Provision

(1) A general regulation on administrative proceedings shall apply to the proceedings under this Act,³⁶⁾ unless otherwise stipulated by this Act.

(2) The general regulation on administrative proceedings shall not apply to

- a) decision-making in the case of doubts under Section 6 Paragraph 5, Section 23 Paragraphs 7 and 10 and Section 25 Paragraph 4,
- b) assessment of data concerning the filing systems submitted for registration (Section 27),
- c) provision of information to the data subject (Sections 20 to 22),
- d) decision-making on objections to bias and notifications of bias (Section 41),
- e) investigation of notifications (Section 45),
- f) proceedings concerning orders (Section 46).

(3) The Office shall make a notice on the state of protection of personal data public on its website after its reading in the National Council of the Slovak Republic.

I n t e r i m p r o v i s i o n s

Section 52

(1) The controllers of the already existing filing systems shall harmonize these systems with this Act within six months from the day of its effectiveness and if required by the Act they shall submit them for registration within the same time limit.

(2) The controllers processing personal data pursuant to a special Act, which does not regulate the requirements under Section 7 Paragraphs 3, 5, 6 or under Section 9 Paragraph 1

³⁶⁾ Act No. 71/1967 Coll. on Administrative Proceedings (Administrative Procedure Code).

Subparagraph a), may process personal data in the extent necessary for achieving the determined purpose of the processing without consent of data subjects until 31 December 2005.

Section 53

(1) Obligations of the authority of the State supervision of personal data protection in filing systems arising from the regulation currently in force shall be transferred to the Office as of the day of effectiveness of this Act.

(2) The rights and obligations arising from employment relationships of the Commissioner for protection of personal data in filing systems and employees of the Inspection Unit of Personal Data Protection under the Governmental Office of the Slovak Republic shall be transferred in full extent to the Office as of the day of effectiveness of this Act.

(3) The State property under administration of the Governmental Office of the Slovak Republic procured for the purposes of fulfilment of the tasks of the State supervision of personal data protection in filing systems shall be transferred to the administration of the Office as of the day of effectiveness of this Act.

(4) The Governmental Office of the Slovak Republic shall provide financial and technical operation of the Office until 31 December 2002.

(5) The State property under administration of the Statistical Office of the Slovak Republic procured for the purposes of registration of filing systems containing personal data shall be transferred to the administration of the Office as of the day of effectiveness of this Act.

(6) The obligations arising for the Commissioner for protection of personal data in filing systems from international treaties in the field of personal data protection shall be transferred to the Office as of the day of effectiveness of this Act.

Section 54

(1) The Commissioner for protection of personal data in filing systems, which was appointed to the function pursuant to the regulation currently in force shall become the President of the Office as of the day of effectiveness of this Act and he shall stay in this function until termination of the term of office for which he was appointed as the Commissioner for protection of personal data in filing systems.

(2) The President of the Office shall decide, in a time limit of two months from the day of effectiveness of this Act, whether the filing system submitted for registration pursuant to the regulations currently in force can be deemed registered under this Act. If the President of the Office decides that such filing system is not subject to registration, the Office shall notify the controller of it in the same time limit.

(3) The proceedings initiated before the day of effectiveness of this Act shall be terminated pursuant to the regulations currently in force.

Section 55

Interim Provisions to the Regulations Effective as of 1 May 2005

(1) The Office for Personal Data Protection under the regulations currently in force shall become the Office for Personal Data Protection of the Slovak Republic pursuant to this Act. In the case when other legal regulations use the term “Office for Personal Data Protection” in all grammatical forms, it shall mean “Office for Personal Data Protection of the Slovak Republic” in the respective grammatical form.

(2) A written authorization of the personal data protection official issued under the regulations currently in force shall be deemed a written authorization under this Act, provided that the personal data protection official fulfils the conditions stipulated in Section 19 Paragraph 12. The controller shall notify the Office, until 30 June 2005, of the data under Section 19 Paragraph 5 and submit a certificate or declaration confirming that the personal data protection official was professionally trained.

(3) The personal data protection official, who was authorized in writing for internal supervision of personal data protection under the regulations currently in force and does not fulfil the conditions stipulated in Section 19 Paragraph 12, must be recalled from the function of a personal data protection official until 30 June 2005 and the controller shall be obliged to authorize in writing another personal data protection official for execution of the internal supervision. This shall not affect the provision of Section 19 Paragraph 5.

(4) The controllers of the already existing filing systems, to which special registration under Section 27 did not apply pursuant to the regulations currently in force, shall be obliged to submit them for a special registration until 30 June 2005, otherwise the right to processing of personal data in these filing systems shall expire by expiration of this time limit.

(5) The President of the Office shall decide until 31 December 2005 whether the filing system submitted for registration and registered under the regulations currently in force can be deemed registered under this Act. If the President of the Office decides that such filing system is not subject to registration under this Act, the Office shall cancel registration of the filing system and, in the same time limit, make the registration numbers of the filing systems, whose registration was cancelled, public on its website.

(6) The proceedings initiated and not terminated by a final decision before effectiveness of this Act shall be terminated under the regulations currently in force. Legal effects of the actions taken within the proceedings before effectiveness of this Act shall be maintained.

(7) Provisions of the regulations currently in force shall apply to the time limits, which did not expire until the day of effectiveness of this Act.

(8) The controllers of the already existing filing systems shall be obliged to harmonize them with this Act until 31 October 2005. This shall not affect Paragraphs 2 to 4.

Final Provisions

Section 56

Transfer of Rights

The term “Commissioner for protection of personal data” referred to in the legal regulations shall mean the “President of the Office” under this Act.

Section 56a

This Act shall implement the Directive of the European Communities and the European Union referred to in the Annex.

Section 57

Repealing Provision

The following shall be repealed:

1. The Act No. 52/1998 Coll. on Protection of Personal Data in Filing systems, as amended by the Act No. 241/2001 Coll.,
2. Regulation of the Statistical Office of the Slovak Republic No. 155/1998 Coll. regulating details concerning the manner, form and procedure of registration of filing systems containing personal data.

Section 58

Effectiveness

This Act shall become effective on 1 September 2002, except for Section 35 Paragraph 2, which shall become effective on 1 December 2003.

Act No. 602/2003 Coll. became effective on 1 January 2004.

Act No. 576/2004 Coll. became effective on 1 January 2005.

Act No. 90 /2005 Coll. became effective on 1 May 2005.

R u d o l f S c h u s t e r by his own hand

J o z e f M i g a š by his own hand

M i k u l á š D z u r i n d a by his own hand

LIST OF THE IMPLEMENTED REGULATIONS
OF THE EUROPEAN COMMUNITIES AND THE EUROPEAN UNION

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 (Ú. v. ES, L 281, 23 November 1995), as amended by the Regulation (EC) No. 1882/2003 of the European Parliament and of the Council of 29 September 2003 (Ú. v. EÚ L 284, 31 October 2003)