THE NATIONAL COUNCIL OF THE SLOVAK REPUBLIC

ACT
№ 428
of 3 July 2002
on personal data protection

The National Council of the Slovak Republic has enacted this law:

P A R T O N E

BASIC PROVISIONS

Subject-matter and scope of the Act

Section 1

(1) This Act shall regulate

a) the protection of natural person's personal data during their processing,

b) principles of personal data processing,

c) personal data security,

d) protection of data subject's rights,

e) transborder personal data flow,

f) registration and record-keeping of information systems,

g) establishment, status and scope of the Personal Data Protection Office (hereinafter the „Office").

(2) This Act shall apply to state administration authorities, bodies of territorial self-governments, other public authorities and also other legal entities and natural persons who process personal data, determine the purpose and means of processing or provide personal data for processing.

Section 2

(1) This Act shall not apply to the protection of personal data processed by a natural person in the course of a purely personal or household activity.

(2) When personal data are processed by a state administration authority or another state authority and their processing is necessary for ensuring an important state interest while this necessity is explicitly laid down in a separate law[1)] in the area of

a) internal order and security,

b) defence,

c) protection of classified information,

d) prosecution and criminal proceedings, protection of economic or financial interests of the State including currency, budgetary and tax issues, or

f) protection of data subject or rights and freedoms of other persons in matters specified under subparagraphs a) to e),

provisions of Section 5 paragraph 4, Section 6 paragraph 3 and 4, Section 7 paragraph 1, 6, 11 to 13, Section 10 paragraph 1 and 8, Section 11 to 14, Section 15 paragraph 4 and 5, Section 16, Section 18 paragraph 1 and 2, Section 20 paragraph 1, Section 23 paragraph 1 to 7, Section 25 to 28 and Section 32 of this Act shall not be applied.

Definition of certain terms

Section 3
Personal data

Personal data shall mean data relating to an identified or identifiable natural person, where such a person is one who can be identified, either directly or indirectly, in particular by reference to a generally usable identification number or to one or more features or attributes specific to his physical, physiological, mental, economic, cultural or social identity.

Section 4

(1) For the purposes of the present Act

a) processing of personal data shall mean any operation or set of operations which is performed upon personal data e.g. their acquisition, collection, recording, organisation, adaptation or alteration, retrieval, browsing, re-organisation, combination, displacement, use, storage, liquidation, transfer, provision, accessibility or disclosure.

b) the provision of personal data shall mean the delivery of personal data for the processing to other legal person, natural person, or an entity abroad other than the data subject, controller, processor or an authorised person,

---

[1)] Section 1 of National Council of the SR Act No. 171/1993 Coll. on the Police Force as amended by Act No. 490/2001 Coll., Sections 1 and 2 of National Council of the SR Act No. 198/1994 Coll. on Military Intelligence Service, Sections 2 and 3 of Act No. 124/1992 Coll. on Military Police, Sections 1 and 2 of National Council of the SR Act No. 46/1993 Coll. on the Slovak Intelligence Service as amended by Act No. 256/1999 Coll., Section 2 of National Council of the SR Act No. 3/1993 Coll. on the establishment of Armed forces of the Slovak Republic as amended, Section 12 of National Council of the SR Act No. 42/1994 Coll. on civil protection of the population as amended, Act No. 241/2001 Coll. on the protection of classified information and on amending and supplementing certain other acts, Sections 3 and 4 of Act No. 153/2001 Coll. on the Prosecution, Sections 1 to 3 of Act No. 335/1991 Coll. on courts and judges as amended, Section 3 of Act No. 440/2000 Coll. on fiscal control administrations, Section 10 of Act No. 367/2000 Coll. on the protection against the legalisation of proceeds of crime and on amending and supplementing certain other acts.

c) the accessibility of personal shall mean the disclosure of personal data or enabling access to them for another legal entity, natural person or an entity abroad other than the data subject, controller, processor or an authorised person,

d) disclosure of personal data shall mean publishing, communicating or displaying personal data in the public by means of mass media, publicly accessible computer networks, public performance or display of works[2)], public announcement, publishing in a public directory, register or descriptive data set[3)], their placing on an official board or other publicly accessible place,

e) liquidation of personal data shall mean dismantling, erasing or physically destroying material carriers in such a way that personal data cannot be reproduced from them,

f) blocking of personal data shall mean bringing personal data in such a condition in which they are inaccessible and any handling with them is prevented,

g) information system shall mean any set, system or database containing one or more personal data that are processed in order to achieve the purpose under separate organisational conditions with the use of automated or non-automated processing means, e.g. file, list, register, descriptive data set, record or a system containing files, documents, contracts, certificates, opinions, evaluations, tests,

h) the purpose of personal data processing shall mean a clearly defined or determined purpose of personal data processing linked with a certain activity in advance,

i) data subject's consent shall mean any free and articulate manifestation of will through which the data subject expresses his/her consent with the processing of his/her personal data,

j) transborder personal data flow shall mean the transmission of personal data outside the territory of the Slovak Republic to entities seated or having permanent residence abroad, or the exchange of this data with such entities,

k) data made anonymous shall mean personal data modified to a form in which it cannot be associated with the data subject,

l) the address shall mean a set of data concerning the residence of a natural person that include the name of the street, number of the house and/or indication number in the register of houses, name of the municipality, and or the part of the municipality, postal area code, name of the district, name of the state,

m) identifier of general application shall mean a permanent identification personal data of the data subject that ensures uniqueness in the information systems,

n) biometric data shall mean personal data of natural persons on the basis of which he/she can be clearly and uninterchangeably identified e. g. finger print, palm print, deoxyribonucleic acid analysis, deoxyribonucleic acid profile,

o) the audit of the information system security shall mean an independent expert assessment of the reliability and overall security of the information system with respect to ensuring confidentiality, integrity and accessibility of processed personal data.

---

2) Section 13 of Act No. 383/1997 Coll. the Copyright Act and act amending and supplementing the Customs Code as amended.

3) E.g. Sections 27 to 34 of the Commercial Code, Sections 8 and 68 of National Council of the SR Act No. 162/1995 Coll. on the real estate registry and entry of ownership and other rights to real estates (the Cadastre Act) as amended by Act No. 255/2001 Coll., Section 26 paragraph 2 subparagraph e) of Act No. 195/2000 on telecommunications.

(2) A controller shall mean a state administration authority, territorial self-government body, other public authority or other legal entity or natural person, which determines the purposes and means of processing. When the purpose and the means of personal data processing are stipulated in a separate law then the controller is that entity the law identifies or the one who complies with the requirements determined by law.

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

(4) An authorised person shall mean any natural person who comes into contact with personal data as a part of his or her employment contract or similar working relation, civil service or public office who may process personal data only on the basis of an instruction by the controller or processor save a separate law provides otherwise.

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

(6) A user shall mean any legal entity or natural person or an entity abroad, which has access to personal data from the information system.

P A R T T W O

RIGHTS, DUTIES AND RESPONSIBILITY IN PROCESSING OF PERSONAL DATA

C H A P T E R O N E

PRINCIPLES OF PERSONAL DATA PROCESSING

Section 5
Controller and processor

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

(2) The processor is only authorised to process personal data in the scope and under the conditions negotiated with the controller in a written contract or a written authorisation.

(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) Only those entities, which have a seat or permanent residence in the territory of Slovak Republic can be controllers and processors.

Section 6
Purpose of data processing

(1) When no separate law stipulates the purpose of data processing, prior to the commencement of processing, the controller shall clearly define the purpose and ensure that personal data which

a) are incompatible with the purpose of processing due to their extent and content while further processing of personal data for historic, statistical and scientific purposes shall not be considered incompatible or

b) are obsolete for the purpose of processing with respect to the time aspect or substance

are not processed.

(2) The purpose of personal data processing must be clear ands shall not contradict the laws.

(3) Only such personal data the extent and content of which complies with the purpose of their processing may be processed. The manner in which personal data are processed and used must comply with the purpose of their processing.

(4) Only such personal data that are necessary to achieve the purpose of their processing can be required from the data subject. The controller or processor may add other data subject's personal data that are directly linked with the purpose of processing only when the data subject was notified and gave a written consent. Neither the controller nor the processor may force such 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.

(5) In case of doubt the Office shall decide whether the extent, content and manner of processing or use of processed data is in compliance with the purpose of their processing or whether they are obsolete with respect to time and substance. The opinion of the Office shall be binding.

Section 7
Data subject's consent

(1) The processing of personal data may only be performed with the data subject's consent. The controller shall ensure demonstrability of the consent in such a way that a proof thereon can be presented.

(2) The evidence of demonstrable consent shall include mainly data on the person who gave the consent, on who received this consent, its purpose, the list of personal data, the period of validity of the consent and conditions for its withdrawal. The written consent without an autograph of the person issuing the consent shall be deemed invalid. An electronic signature under a separate law may be used for an electronic document for this purpose.

(3) Consent under paragraph 1 shall not be required when the personal data are processed on the basis of a separate law[4)] that lays down a list of personal data, the purpose of their processing, conditions for their acquisition and the group of data subjects.

(4) Consent under paragraph 1 shall not be requested when

a) personal data are processed, without a possibility of providing them and making them accessible, exclusively for the purposes of scientific, artistic and literary works, for the needs of informing the public via mass media and also historic or scientific purposes and when the processing is made by a controller who has this obligation as a result of his/her business activity,

b) the processed personal data are used for statistical purposes; in these cases personal data have to be made anonymous,

c) personal data processing is necessary for the protection of vital interests of a data subject who has no legal capacity or is physically incapable to give consent and when no consent of his/her representative at law can be acquired,

d) the subject of processing is exclusively the title, name, surname and address of the data subject without a possibility of associating other personal data, and they should be used exclusively for the needs of the controller in postal communication with the data subject and the record-keeping of these data; when controller's business is direct marketing these personal data can be provided only when they are given to another controller that has the same business exclusively for the purposes of direct mailing without a possibility of access and disclosure and the data subject did not object in writing under Section 20 paragraph 3 subparagraph c) or

e) already disclosed personal data are processed; in these cases personal data have to be marked appropriately.

(5) Person different than the data subject except persons under paragraphs 8 and 9 can give personal data of a data subject to an information system only with his/her written consent. This shall not apply when it is necessary for criminal justice agencies to perform their tasks or when personal data are supplied to an information system on the basis of a separate law[5)] that lays down a list of personal data, purpose of their processing and conditions for their supply.

(6) Processed personal data of the data subject can be given, made accessible or published only with his/her written consent. This shall not apply when it is necessary for the performance of tasks of criminal justice agencies or when personal data are give, made accessible or published from information systems on the basis of a separate law[6)] that lays down a list of personal data, purpose and conditions of providing, making accessible or publishing personal data and also legal entities, natural persons or entities abroad that are personal data provided or made accessible.

[4)] E.g. Sections 38 to 41 of National Council of the SR Act No. 387/1996 Coll. on employment, Section 11a paragraph 2 of National Council of the SR Act No. 542/1990 Coll. on state administration in the school system and on school self-administration as amended by Act No.. 416/2001 Coll. on the transfer of some competencies from state administration bodies to municipalities and higher territorial units.

[5)] E.g. Section 17 and paragraph 15 of the general part of Annex 5 to Act No. 241/2001 on the protection of classified information and on amending and supplementing certain other laws.

[6)] E.g. Section 11 paragraph 3 of Act of the Slovak National Council No. 542/1990 Coll. as amended, Section 20 of Act No. 241/2001 Coll.

(7) The one who intends to disclose data subject's personal data must not interfere with the right to the protection of their personhood and privacy in an unauthorised way; their disclosure must not be in contradiction with data subject's justified interests[7)].

(8) When the data subject has no full legal capacity [8)] the consent required under this law can be given by his/her representative at law[9)].

(9) When the data subject is deceased the consent required under this law can be given by his/her significant other[10)]. The consent shall not be valid when as few as one significant other gave his/her disapproval in writing.

(10) Where the processed personal data are a part of a valid contract, where one of the parties is the data subject, and which includes particulars under paragraph 2, the signature of the data subject on the contract shall at the same time express the written consent with personal data processing.

(11) Data subject's personal data can be given from the information system to another legal entity, natural person or an entity abroad only with a written document of the consent given where this Act requires such consent; the one who gives personal data in this way may substitute the written document of consent with controller's written statement of consent given by data subjects when the controller can prove that data subjects' written consent was given.

(12) Personal data under paragraph 4 subparagraph c) and under Section 9 paragraph 1 subparagraph b) can be processed without the consent of the data subject only for such a period of time during which grounds preventing the acquisition of data subject's consent exist. When the grounds cease to exist the one who is processing personal data shall acquire data subject's consent.

(13) The one who claims to be processing disclosed personal data should, upon request, prove the Office that the processed personal data have already been disclosed.

(14) The user may process accessible data subject's personal data only for his/her own need in the course of a purely personal or household activity.

Section 8
Special categories of personal data

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

(2) An identifier of general application laid down by a separate law[11)] may be used for the purposes of determination of the natural person in personal data processing only when its use shall be necessary for achieving the purpose of processing. Processing another identifier that

---

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) Act of the National Council of the Slovak Republic No. 301/1995 Coll. on birth identification number.

contains characteristics of data subject or disclosing an identifier of general application shall be prohibited.

(3) Processing of personal data relating to violations of criminal law, administrative law or civil law provisions as well as the enforcement of final judgements or decisions may be performed only by those ones who are covered by a separate law[12)].

(4) Biometric data may be processed only under conditions laid down in a separate law when

a) it is explicitly provided so for the controller by law or
b) the data subject gave his/her consent to processing in writing.

(5) Processing of personal data relating to mental identity of natural person or his/her mental fitness for work can be performed only by a psychologist or by those ones who are covered by a separate law [13)].

Section 9
Exemptions from restrictions
while processing of special categories of personal data

(1) The prohibition of personal data processing laid down in Section 8 paragraph 1 shall not apply when the data subject gave his/her written consent with their processing or

a) a separate law that lays down a list of personal data, the purpose of their processing, conditions for their acquisition and the group of data subjects requires processing or

b) processing is necessary for the protection of vital interests of a data subject or of another natural person who has no legal capacity or is physically incapable to give consent and when no consent of his/her representative at law can be acquired or

c) processing is performed by a civil association, foundation or non-profit organisation providing generally beneficial services, political party or political movement, trade unions, church or religious society recognised by the State in the framework of its authorised activity and this processing applies only to their members who are in regular contact with them considering their objectives and personal data are purely used for their internal needs or

d) processing applies to personal data the data subject disclosed or that are necessary for enforcing his/her legal claim or

e) the processing is required for the purposes of preventive medicine, medical diagnosis, sickness insurance and social security, provision of medical treatment or for the purpose of health care services and these data are processed by a health care facility, health insurance company or the Social Insurance Company.

(2) Data subject's written consent given under paragraph 1 shall be invalid when a separate law excludes it.

---

12) E.g. Section 40 paragraph 2 subparagraph d) of Act No. 153/2001 Coll., Section 52 of National Council of the SR Act No. 372/1990 Coll. on infractions as amended, of National Council of the SR Act No. 171/1993 Coll. as amended.

13) E.g. Sections 2 of National Council of the SR Act No. 199/1994 Coll. on psychological services and the Slovak chamber of Psychologists, National Council of the SR Act No. 542/1990 Coll. on state administration in the school system and on school self-administration as amended .

(3) Provision of Section 8 paragraph 4 shall not be applied when biometric data with the exception of deoxyribonucleic acid analysis and deoxyribonucleic acid profile of data subjects are processed for the purposes of registering entry or access to closed areas and when it is a purely internal need of the controller.

Section 10
Acquisition of personal data

(1) The authorised person who acquires personal data on behalf of the controller or processor shall produce proof of his/her identity at the request by those from whom he/she requires data subject's personal data and shall notify him/her, without being called to do so, in advance of

a) the name and seat or permanent residence of the controller; if a processor is acting on behalf of the controller then also his/her name and seat or permanent residence,

b) of the purpose of personal data processing determined by the controller or laid down by a separate law; acquisition of personal data under the pretext of another purpose or another activity shall be excluded,

c) the voluntary or obligatory basis of providing the required personal data,

d) the law that lays down the obligation to provide the required personal data and the consequences of refusing to do so,

e) the range of users who will have access to personal data,

f) legal entities, natural persons or entities abroad who will be given personal data,

g) the form of disclosure if the personal data are to be disclosed,

h) countries of transborder flow of personal data.

(2) The authorised person who acquires personal data on behalf of the controller or processor under paragraph 1 subparagraph d) shall produce proof of his/her authorisation for such activity in case it is not laid down by a law.

(3) The authorisation for the acquisition of personal data shall be issued either by the controller or processor.

(4) The controller who acquires personal data for the purposes of identifying a natural person for a single entry of its premises is authorised to ask the name, surname, title and identity card number[14)] or service card number or travel document number[15)], nationality and to verify the veracity of the given personal data against the presented document. When the natural person identifies himself/herself under a separate law[16)] the controller shall be authorised to request only the registration number of the service card. In these cases paragraph 1 shall not be applied.

---

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

(5) The controller or processor who acquires, provides personal data or makes them accessible shall ensure confidentiality of their processing.

(6) Acquisition of personal data necessary for achieving the purpose of processing by copying, scanning or other recoding of official documents on an information carrier shall be possible only when the data subject agrees with it in writing or when a separate law makes this explicitly possible also without data subject's consent[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) Area open to public may be monitored with video-recording or audio-recording purely for the purposes of public order and security, detection of crime or violation of state security and only when the area is clearly marked as monitored area. No marking of monitored area shall be required when laid down so in a separate law. The recording made can be used for the purposes of criminal proceedings or administrative proceedings unless a separate law provides otherwise.

(8) The controller who acquires personal data specified under Section 7 paragraph 4 subparagraph d) without data subject's knowledge or directly from him/her shall give him/her information under paragraph 1 during the first contact and if these data are processed for the purpose of direct marketing he/she shall inform the data subject of his/her right to object, in writing, against their provision and use in postal communication.

(9) Those controllers whose business is direct marketing shall keep a list of provided personal data under Section 7 paragraph 4 subparagraph d) identifying the name, surname, title and address of data subject, date of their supply, or, if applicable, the date from which it is prohibited to supply them under section 13 paragraph 6 and the name of legal entity or natural person who was provided the concerned personal data. Legal entities and natural persons who were provided these personal data shall keep a list of the same scope.

Section 11
Veracity of personal data

Only true personal data may be supplied to an information system. The one who has provided personal data to the information system shall be responsible for their lack of veracity.

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) For the purpose of accurate and up-to-date nature of personal data the controller shall ensure correcting or supplementing those personal data that have become obsolete or lack of accuracy has been proved during processing.

Section 13

[17] Section 15 paragraph 3 of Act No. 200/1998 Coll. on civil service of customs officers as amended and on amending and supplementing certain other acts.

Liquidation of personal data

(1) After achieving the purpose of processing the controller shall ensure liquidation of personal data without delay.

(2) The controller shall ensure the liquidation of personal data without delay except for personal data laid down in Section 7 paragraph 4 subparagraph d) also when

a) the grounds preventing acquisition of data subject's consent (Section 7 paragraph 12) extinct and consent was not given or

b) the data subject has put forward an objection under Section 20 paragraph 3 subparagraph a); the controller shall continue to act according to paragraph 5.

(3) Paragraph 1 shall not be applied when

a) a separate law stipulates a time limit[18)] that prevents liquidation of personal data without delay; the controller shall ensure personal data liquidation after the expiration of the time limit laid down by law immediately,

b) personal data are a part of archival documents[19)],

c) written, visual, audio or other recordings containing personal data shall be included into pre-archival care[20)]; during the pre-archival care no processing operations with the data may be performed except their storage and they may be used solely for the purposes of civil proceedings, criminal proceedings or administrative proceedings.

(4) Storage periods of written, visual, audio and other recordings containing personal data and included into pre-archival care can be imposed only for the period of time necessary for claiming rights or exercising duties laid down by law[21)].

(5) If the data subjects puts forward an objection under Section 20 paragraph 3 subparagraph b) the controller shall immediately terminate the use of personal data specified in Section 7 paragraph 4 subparagraph d) in postal communication.

(6) If the data subject submits an objection under Section 20 paragraph 3 subparagraph c) the controller shall inform in writing everyone who was supplied personal data specified in Section 7 paragraph 4 subparagraph d) of this without delay; the prohibition of further providing these specified personal data shall apply to the controller and everyone the controller provided it to from the day following the day of data subject's objection service or service of controller's written notification.

(7) If the recording made under Section 10 paragraph 7 is not used for the purposes of criminal proceedings or administrative proceedings the one who made it shall liquidate it not later than seven days from the day following the day on which the recording was made provided a separate law does not stipulate otherwise.

---

18) E.g. sections 31 and 32 of Act No. 563/1991 Coll. on accounting as amended by Act No. 336/1999 Coll.

19) Section 2 paragraph 1 Act of the National Council of the Slovak Republic No. 149/1975 Coll. on archival services as amended by act No .571/1991 Coll.

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

21) For instance Sections 101 to 110 of the Civil Code.

(8) The controller shall ensure liquidation of those personal data that cannot be corrected or supplemented in such a way that they are accurate and up-to-date (Section 12 paragraph 2).

Section 14
Notification of correction or liquidation

(1) The controller shall notify the data subject and everyone who was given data concerned of having them corrected or liquidated within 30 days from execution.

(2) A notification may be waived when lack of notifying the correction or liquidation of personal data will not result in violation of data subject's rights.

C H A P T E R T W O
Security of personal data

Section 15
Responsibility for personal data security

(1) The controller and processor shall be responsible for the security of personal data by protecting them against stealing, loss, damage, unauthorised access, alteration and dissemination. Appropriate technical, organisational and personal measures corresponding the manner of processing shall be taken to this end.

(2) The controller and processor shall adopt measures under paragraph 1 in the form of information system security project (hereinafter only „security project") and they shall ensure its development when

a) the information system is connected to a publicly accessible computer network or is operated in a computer network that is connected to a publicly accessible computer network,

b) special categories of personal data (Section 8) are processed in the information system or

c) the information system is subject to exemptions under Section 2 paragraph 2.

(3) Upon Office's request the controller and processor shall demonstrate the scope and content of adopted technical, organisational and personnel measures under paragraph 1 or 2.

(4) When information systems under paragraph 2 are the subject of inspection the Office shall have the right to require the controller or processor to present an evaluation report of the information system security audit result (hereinafter the „evaluation report") in case of serious doubts concerning its security or practical application of measures laid down in the security project. The controller or processor shall immediately submit the Office the evaluation report that is not older than two years; otherwise, he/she shall arrange an information system security audit at his/her own costs and submit the evaluation report not later than three months from the imposition day of this obligation.

(5) The information system security audit can only be made by a qualified legal entity or natural person who was not participating in the drafting of the security project of the concerned information system and there are no doubts as to his/her impartiality.

Section 16
The security project

(1) The security project defines the scope and manner of technical, organisational and personnel measures needed for eliminating and minimising the threats and risks affecting the information system with respect to violating its security, reliability and functionality.

(2) The security project shall be drafted in compliance with the basic rules of information system security, published security standards, regulations and international treaties binding upon the Slovak Republic.

(3) The security project shall include mainly

a) security plan,

b) information system security analysis,

c) security guidelines.

(4) The security plan shall define basic security objectives that must be achieved to protect the information system against threat to its security and it includes mainly

a) formulation of basic security objectives and minimum required security measures,

b) specification of technical, organisational and personal measures to ensure protection of personal data in the information system and the manner of their use,

c) definition of the information system environment and its relation to a potential security violation,

d) definition of borders determining the set of residual risks.

(5) Information system security analysis shall present a detailed information system security analysis that includes mainly

a) the qualitative analysis of risks in the framework of which threats affecting the individual assets of the information system capable of violating its security or functionality are identified; the result of the qualitative analysis is a list of threats that can imperil confidentiality, integrity and accessibility of personal data together with the identification of the potential scope of the risk, proposal of measures eliminating or minimising the effect of risks and the definition of the list of uncovered risks,

b) using security standards and definition of other methods and means of personal data protection; the conformity assessment of proposed security measures with the security standards, methods and means is a part of the information system security analysis.

(6) Security guidelines detail out and apply the conclusions resulting from the security project to concrete conditions of the operated information system and they include mainly

a) the description of technical, organisational and personnel measures defined in the security project and their use under concrete conditions,

b) the scope of authorisations and description of permitted activities by individual authorised persons, the manner of their identification and authentication when accessing the information system,

c) the scope of responsibility of authorised persons and the person responsible for overseeing the protection of personal data (Section 19),

d) the manner, form and frequency of inspection focusing on the observance of information system security,

e) procedures in case of breakdowns, failures and other contingencies including preventive measures to reduce the occurrence of contingencies and the possibility of effective restoration of the situation prior to the breakdown.

Section 17
Instruction

The controller and processor shall instruct legal entities and natural persons who have or can have access to the information system about their rights and obligations provided hereunder and the liability for breaching them, in a demonstrable way.

Section 18
Confidentiality obligation

(1) The controller and the processor shall be obliged to maintain the confidentiality of any personal data processed by them. The obligation of confidentiality shall also extend beyond the end of processing. The obligation of confidentiality shall not apply when, under a separate law, it is necessary for the fulfilment of criminal justice agencies tasks; this is without any prejudice to the provisions of separate laws[22)].

(2) An authorised person shall have the obligation to maintain the confidentiality of any personal data he/she comes across; he/she may not use the data for his/her personal use, neither may he/she disclose them, give them nor make them accessible to anyone without controller's consent.

(3) The obligation of confidentiality under paragraph 2 shall also apply to other natural persons, who as a part of their activities (e.g. maintenance and servicing of technical means) come across personal data at controller's or processor's site.

(4) The obligation of confidentiality under paragraph 2 shall also continue after authorised person's function end or after the termination of his/her employment or a similar relation, civil service or a relation under paragraph 3.

(5) The provisions of paragraphs 1 to 4 and the stipulated obligation of confidentiality by controllers, processors and authorised persons under separate regulation[23)] shall not apply with respect to the Office when fulfilling its mission (Sections 38 to 44).

---

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

23) E.g. Section 6 paragraph 1 of Act No. 150/2001 Coll. on tax authorities amending and supplementing Act No. 440/2000 Coll. on fiscal control administrations, Section 14 of Act No. 330/2000 Coll. on the stock exchange, Section 134 of Act No. 566/2001 Coll. on securities and investment services and on amending and supplementing certain other acts (the Securities Act), Sections 91 to 93 of Act No. 483/2001 Coll. on banks and on amending and supplementing certain other acts, Section 24 of Act No. 24/1991 Coll. on insurance services as amended, Section 81 subparagraph e) and Section 240 paragraph 5 of Act No. 311/2001 Coll. Labour Code, Section 53 paragraph 1 subparagraph e) of Act No. 312/2001 Coll. on civil service as amended, Section 9 paragraph 2 subparagraph b) Act No. 313/2001 Coll. on public service, Section 8 of Act No. 367/2000 Coll.,

Section 19
Personal data protection supervision

(1) Under this Act the controller shall be responsible for the supervision of personal data protection.

(2) If the controller employs more than five persons he/she shall task in writing a responsible person or several responsible persons who will oversee the compliance with the law in personal data processing.

(3) The controller shall ensure training of the responsible person or several responsible persons. The scope of training shall mainly comply with the content of this Act and tasks resulting from it as well as the content of international treaties on personal data protection [24)], that were promulgated in the way as laid down by law. The Office may request the controller to submit evidence of performed training.

(4) Prior to processing personal data in the information system the responsible person shall assess whether the processing presents a risk of violating data subject's rights and freedoms. The responsible person shall, without any delay, inform the controller of any violations of rights and freedoms of data subjects determined prior to processing or of any violation of legal provisions during the processing of personal data in writing; if the controller fails to immediately remedy the situation the responsible person shall notify the Office.

C H A P T E R T H R E E
PROTECTION OF DATA SUBJECT'S RIGHTS

Section 20
Data subject's rights

(1) A data subject shall have the right to request in writing from the controller

a) information about the situation in the processing of his/her personal data in the information system in the scope under Section 26 paragraph 3,

b) accurate information concerning the source from which personal data processed under Section 7 paragraph 4 subparagraph d) and e) were acquired,

c) a copy of his/her personal data that are the subject of processing,

d) correction of incorrect or obsolete personal data in the course of processing,

e) liquidation of his/her personal data when the purpose of processing was achieved under Section 13 paragraph 1; when official documents containing personal data are the subject of processing he/she may ask for their return,

---

Section 80 Act of the National Council of the Slovak Republic No. 171/1993 Coll. as amended, Section 15 paragraph 2 and 3 Act of the National Council of the Slovak Republic No. 38/1993 Coll. on the organisation of the Constitutional court of the SR and proceedings before the Constitutional Court and the status of its justices.

[24)] E.g. the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Notification No. 49/2001 Coll.).

f) liquidation of his/her personal data that are the subject of processing in case of law violation.

(2) The right of a data subject may only be restricted by virtue of paragraph 1 subparagraphs d) and e) if such a restriction results from a separate law or its application would violate the protection of a data subject or the rights and freedoms of any other persons.

(3) A data subject shall have the right to object on the basis of a written request free of charge against

a) the processing of any of his/her personal data which he/she expects to be processed for the purposes of direct marketing without his/her consent and to demand their liquidation,

b) the use of personal data under Section 7 paragraph 4 subparagraph d) for the purposes of direct marketing in postal communication or

c) supplying personal data under Section 7 paragraph 4 subparagraph d) for the purposes of direct marketing in postal communication or

(4) A data subject shall have the right to object and not to be subject to any decision by the controller which would have legal effects on or would have significant consequences for him/her when such a decision is made solely on the basis of automatic processing of his or her personal data. This right may only be restricted if provided so by a special law[25)] in which measures to ensure the legitimate interests of a data subject are laid down or the restriction of a right results from a contract concluded between the controller and data subject.

(5)The data subject shall have the right to disagree with the notification under Section 23 paragraph 5 and to refuse, in writing, the transfer of his/her personal data

a) to entities with their seat or permanent residence abroad with the exception of the entity identified under subparagraph b); and even this only in case the country of destination guarantees an appropriate level of protection, or

b) to the organisational component of the controller or its superior body in case the country of destination fails to guarantee appropriate level of protection and the transfer can be conducted only with data subject's consent.

(6) After discovering that his/her personal data are subject of unauthorised processing, the data subject may notify the Office of this fact.

(7) If the data subject has no full legal capacity[8)], his/her representative at law may exercise his/her rights[9)].

(8) If the data subject deceased his/her rights under this Act can be claimed by his/her significant other[10)].

Section 21
Provision of information to data subject

25) E.g. Sections 121 and 122 of Act No. 100/1988 Coll. on social security as amended.

(1) The controller hall satisfy data subject's requirements under Section 20 paragraph 1 subparagraphs a), d) to f) free of charge.

(2) A controller shall provide a data subject with information as defined under Section 20 paragraph 1 subparagraphs b) and c) free of charge with the exception of a payment that may not exceed the amount of material costs linked with the making of copies, acquisition of technical carriers and sending the information to the data subject provided a separate law does not stipulate otherwise[26)].

(3) The controller shall satisfy the requirements of a data subject under Section 20 and inform him/her in writing no later than 30 days from receiving them.

Section 22
Notification of the restriction of data subject's rights

The controller shall inform the data subject and the Office of the restriction of data subject's rights under Section 20 paragraph 1 subparagraphs d) and e) without delay.

C H A P T E R F O U R

TRANSBORDER PERSONAL DATA FLOW

Section 23

(1) When the country of destination guarantees an adequate level of protection data transfer to an entity with its seat or residence abroad can be conducted provided requirements under Section 10 paragraph 1 were satisfied.

(2) The adequacy of the level of protection of personal data shall be assessed on the basis of all the circumstances surrounding a data transfer operation. Particular consideration shall be given to the laws in the country of final destination with respect to the nature of personal data, their purpose and duration of the proposed processing operation.

(3) If the country of destination does not satisfy requirements under Section 10 paragraph 1 transfer under paragraph 1 can be carried out only when

a) it is transfer of personal data processed under Section 7 paragraph 4 subparagraph d); this shall apply only when the entity is an organisational component of the controller or its superior body that will not give or make accessible these personal data to another entity in the country of destination with the exception of such an entity that is processing them on behalf of the controller,

b) the transfer is laid down by a separate law, or

c) the transfer results from an international treaty binding upon the Slovak Republic.

(4) In case the country of destination fails to assure the appropriate level of protection the transfer can be performed under the condition that

---

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

a) the data subject has given a consent, in writing, to it knowing that the country of destination fails to assure an appropriate level of protection,

b) it is necessary to fulfil the contract between the data subject and the controller or to implement pre-treaty measures upon data subject's request,

c) it is necessary for concluding a contract or fulfilling a contract that has been concluded by the controller with another entity in the interest of the data subject,

d) it is necessary to fulfil an international treaty binding upon the Slovak Republic or it results from law as an important public interest or it is needed in proving, demonstrating or defending a legal claim,

e) it is necessary for the protection of vital interests of a data subject, or

f) it concerns personal data that are a part of lists, registers or descriptive data sets and that are kept and made publicly accessible according to separate laws or are accessible, according to them, to those who prove a legal claim provided the requirements for making them accessible laid down by law are met.

(5) When the controller decides to transfer personal data only after their acquisition he/she shall notify the data subject the reason for his/her decision prior to their transfer and shall inform him/her of his/her right to refuse such transfer (Section 20 paragraph 5). This shall not apply when it is a transfer under paragraph 3.

(6) When the controller commissions an entity abroad who is processing personal data on behalf of the controller with the processing of personal data then this entity shall be authorised to process personal data only in the scope and under conditions negotiated with the controller in a written contract. The content of this contract must be drafted in compliance with standard contractual conditions laid down for the transfer of personal data to entities abroad who are processing them on behalf of the controller.

(7) Consent by the Office shall be required for the transfer of personal data under Section 6.

(8) The one who performs transfer of personal data shall guarantee their security (Section 15 paragraph 1) also during transit.

(9) The protection of personal data transferred to the territory of the Slovak Republic from entities with a seat or permanent residence abroad shall be performed in compliance with this law.

(10) The Office shall decide on transborder personal data flow in case of doubt. The opinion of the Office shall be binding.

C H A P T E R F I V E

REGISTRATION AND ENTERING IN RECORDS OF INFORMATION SYSTEMS

Section 24
The obligation of registration and entering into records

The controller shall register information systems or shall keep records in the scope and under conditions laid down by this law.

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

Section 25
Conditions of registration

(1) The Office shall perform registration of information systems free of charge.

(2) Information systems in which

a) special categories of personal data (Section 8) are processed,

b) personal data that are the subject of transborder flow (Section 23 paragraphs 1 to 7) are processed, or

c) personal data are processed by a processor (Section 5 paragraph 2)

are subject to registration.

(3) Information systems specified in paragraph 2 shall not be subject to registration if they contain

a) personal data relating to health and an identifier of general application of those persons who have an employment contract or a similar working relations with the controller and of persons who are in civil service relation with the controller,

b) personal data concerning the membership of persons in trade unions which are their members and these personal data are used exclusively for their internal needs,

c) personal data on the religious belief of persons associated in a state recognised church or religious society and when these personal data are used exclusively for their internal needs,

d) personal data concerning the membership of persons in political parties which are their members and when these personal data are used exclusively for their internal needs,

e) personal data of persons taking part in proceedings before a state administration body, territorial self-government body and also before other bodies of public administration and their processing is performed on the basis of a separate law,

f) purely personal data already disclosed ,

g) personal data used by mass media purely for their informing activity,

h) personal data for the purposes of preventive medicine, medical diagnostics, provision of treatment or spa care and other health care service and when these personal data are processed by the health care facility,

i) personal data for the purposes of raising and education or science and research as well as personal data used for the purposes of state statistics and when the controller is a facility given this task by law or

j) personal data that are processed purely for the purposes of identifying persons for their single entry of controller’s premises.

(4) The Office shall decide on registration of the information system in case of doubt. The opinion of the Office shall be binding.

Section 26
Filing for registration

(1) The controller shall be the responsible for filing the information system for registration.

(2) The controller shall file the information system for registration prior to starting personal data processing.

(3) When filing the information system for registration, the controller shall give the following data

a) controller's name, seat or permanent residence, legal form and identification number ,

b) name and surname of controller's authorised representative,

c) the name and surname of the responsible person overseeing the protection of personal data protection if his/her authorisation requires so (Section 19 paragraph 2),

d) the controller's name, seat or permanent residence, legal form and identification number when he/she processes personal data on behalf of the controller,

e) the name and surname of processor's authorised representative,

f) the identification marking of the information system,

g) the purpose of personal data processing,

h) the list of personal data,

i) the group of data subjects,

j) the group of users if personal data are made accessible for them,

k) legal entities, natural persons or entities abroad when they are given personal data,

l) names of countries of destination, legal basis of transborder personal data flow and measures to assure protection of personal data in transit when they are the subject of cross border flow,

m) the legal basis of the information system,

n) the form of disclosure if disclosure of personal data is performed,

o) a general characterisation of measures to ensure personal data protection,

p) the date of beginning personal data processing.

(4) The data in a scope pursuant to paragraph 3 shall be submitted to the Office in a written form, confirmed by the authorised representative of the controller or electronically as a database file with a hard copy of the content confirmed by controller‘s authorised representative. The Office shall determine the written form and the format of the database file. No attached hard copy is required when the database file has an electronic signature under separate law.

Section 27
Preliminary screening and issuance of registration certificate

(1) The Office shall evaluate the submitted data (Section 26 paragraph 3), check whether processing of personal data does not present a risk of violating the rights and freedoms of data subjects and shall issue a binding opinion on the information system registration obligation not later than 30 days from their receipt.

(2) In case of doubt the Office shall require additional explanation from the controller. During this period the time limit under paragraph 1 shall be suspended.

(3) Allocation of a registration number to an information system and issuance of a registration certificate shall be a part of registration. The controller shall always give the registration number in any communication concerning personal data processing.

(4) The controller may start personal data processing in an information system submitted to registration on the day following the day on which the Office issued the registration certificate.

Section 28
Notification of changes and deregistration

(1) The controller shall notify, in writing, the Office of any changes of data under Section 26 paragraph 3 with the exception of subparagraph p) that occur during processing within 15 days.

(2) The controller shall deregister, in writing, within 15 days from the day of terminating personal data processing in the information system. The date of terminating personal data processing is a part of deregistering.

(3) Section 26 paragraph 4 shall be applied to notification of changes and deregistration of the information system as appropriate.

E n t e r i n g i n t o r e c o r d s

Section 29
Requirements for records keeping

(1) The controller shall keep records on those information systems that are not subject to registration from the day of commencing data processing in these information systems the latest.

(2) Paragraph 1 shall not be applied when

a) the processed personal data are purely used for the needs of postal communication with the data subjects and the entering of these data into records [Section 7 paragraph 4 subparagraph d)], or

b) they contain personal data that are processed purely for the purposes of identifying persons for their single entry of controller’s premises (Section 10 paragraph 4).

Section 30
The content of records

Records under Section 29 paragraph 1 shall include data specified in Section 26 paragraph 3.

D e c l a s s i f i c a t i o n o f r e g i s t r a t i o n a n d r e c o r d k e e p i n g

Section 31
The public nature of registration

Registration kept under this Act shall be public in the scope of data under Section 26 paragraph 3 and it shall identify the registration number of the information system.

Section 32
The public nature of record keeping

Record keeping under this Act shall be public. The controller shall make data from the records accessible to anyone requesting them free of charge.

P A R T T H R E E

THE OFFICE

C H A P T E R O N E
THE STATUS AND SCOPE OF THE OFFICE

Section 33
The scope of the Office

(1) The Personal Data Protection Office, which is a body of state administration with a state-wide competence and its seat in Bratislava, shall be established.

(2) The Office, being a state authority, shall oversee the protection of personal data in an independent manner and shall participate in the protection of fundamental rights and freedoms of natural persons in the processing of their personal data.

(3) When personal data are processed by intelligence services the National Council of the Slovak Republic shall oversee the protection of personal data under paragraph 2 according to a separate law. [27)]

Section 34
The status of the Office

(1) The Office shall be a state budget financed organisation[28)]. The Office shall submit its draft budget as a part of the Office of the Government budget title. The National Council of the Slovak Republic can only cut the budget of the Office in the course of a calendar year.

[27)] Section 60 Act of the National Council of the Slovak Republic No. 350/1996 Coll. on the standing order of the National Council of the Slovak Republic .

[28)] Section 21 paragraph 1 and paragraph 4 subparagraph a) Act of the National Council of the Slovak Republic No. 303/1995 Coll. on budgetary rules as amended.

(2) Details concerning the organisation of the Office shall be regulated in the organisational rules.

Section 35
The President of the Office

(1) The Office shall be headed by a President.

(2) The National Council of the Slovak Republic shall elect and recall the President of the Office upon a proposal submitted by the Government of the Slovak Republic. The Government of the Slovak Republic shall submitted the National Council of the Slovak Republic a proposal for the election of the President of the Office for a new term not later than 60 days before the lapse of the term of the acting President of the Office. The term of the office of the President of the Office shall be five years and he/she may be elected for not more than two consecutive terms. The President of the Office shall also stay in the office after the lapse of the term until the National Council of the Slovak Republic elects a President of the Office for a new term.

(3) Only a citizen who could be elected member of the National Council of the Slovak Republic, who is a person of integrity, who has university education, at least 10 years of practice in information sciences or law and is at least 35 years of age can be elected President of the Office.

(4) A citizen who has not been sentenced with a final judgement for a wilful crime or an unconditional deprivation of liberty for a crime shall be considered a person of integrity. Integrity shall be demonstrated with a criminal record statement that is not older than three months.

(5) The President of the Office can neither be a member of a political party nor of a political movement.

(6) The salary and other particulars of the President of the Office shall be determined by the Government of the Slovak Republic under a separate regulation[29)].

(7) During his/her term the President of the Office is not allowed to be engaged in business activities or any other gainful activity with the exception of scientific, teaching, journalistic, literary or artistic activity and the administration of own property and property of his/her minor children.

(8) During his/her term the President of the Office shall be entitled to learn classified information under separate regulation[30)].

(9) During his/her term of the office and also beyond it the President of the Office shall have the obligation to maintain confidentiality of facts relating to personal data protection he/she learned during his/her term of the office.

---

29) Act No. 312/2001 Coll.
30) Section 31 paragraph 1 subparagraph h) of Act No. 241/2001 Coll.

(10) The National Council of the Slovak Republic may lift the confidentiality obligation of the President of the Office for a concrete case.

(11) The President of the office shall be accountable for his/her activity to the National Council of the Slovak Republic.

(12) Prior to the lapse of the term, holding of the office of the President shall cease upon

a) resignation from the office,
b) loss of eligibility for being elected member of the National Council of the Slovak Republic,
c) a judgement finally convicting him/her of a wilful criminal offence or of a criminal offence when the court did not decide on probationary suspension of the imprisonment sentence in his or her case,
d) performance of activity that is incompatible with holding this office or
e) death.

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

a) when his health prevents him from duly performing the duties resulting from his office for a long term, however, at least for the period of a year,

b) when violating the obligation to maintain confidentiality of facts relating to personal data content he/she learned during his/her term of the office.

The President of the Office shall be recalled from the office from the day following the day on which he/she was served the decision of the National Council of the Slovak Republic on recalling him/her from the office.

Section 36
Vice-President of the Office

(1) The Vice-president of the Office shall deputize for the President of the Office during his absence. In addition, the Vice-president of the Office shall perform tasks given to him/her by the President of the Office.

(2) The Government of the Slovak Republic shall appoint and recall the Vice-president of the Office upon a proposal by the President of the Office.

(3) Provisions of Section 35 paragraphs 3 to 5, 7, 9 and 12 shall be applied to the office of the Vice-president of the Office as appropriate.

(4) The National Council of the Slovak Republic may lift the confidentiality obligation of the Vice-president of the Office for a concrete case.

Section 37
Chief inspector and inspectors

(1) Chief inspector shall manage the activities of inspectors.

(2) Inspectors shall carry out inspection tasks and they shall have substantive competence to fulfil the tasks of the Office.

(3) The Government of the Slovak Republic shall appoint and recall the inspectors upon a proposal by the President of the Office. Only a citizen who could be elected member of the National Council of the Slovak Republic, who is a person of integrity, who has university education, at least 3 years of practice in information sciences or law and is at least 30 years of age can be appointed inspector. The Government of the Slovak Republic shall appoint and recall the chief inspector from the ranks of inspectors who have a professional experience of at least five years and the age of at least 35 years upon a proposal by the President of the Office.

(4) The term of the office of the chief inspector shall be five years and he/she may be repeatedly appointed. Paragraphs 2 and 6 and provisions of Section 35 paragraphs 4, 5, 7, 12 and 13 shall apply to the office of the chief inspector as appropriate.

(5) Provisions of Section 35 paragraphs 4, 5, 7, 12 and 13 shall apply to the office of inspector as appropriate. In addition to grounds laid down in Section 35 paragraph 13 an inspector may be recalled for

a) repeated failure to fulfil tasks laid down in Section 38 paragraph 1 subparagraph f) and h) or systematic less serious violations of discipline at work and when the President of the Office repeatedly urged, in writing, the inspector to remove shortcomings in the course of the last six months and the inspector failed to remove them in a reasonable time, or

b) gross negligence of inspector's duty laid down by this Act [Section 38 paragraph 1 subparagraph f) and h)] when he/she failed to prove that it was not his/her fault or that he could not prevent it; or for gross violation of work discipline.

(6) During their employment term and also beyond it inspectors and other employees of the Office shall have the obligation to maintain confidentiality of facts relating to personal data content they learned during their work. The President of the Office may lift the confidentiality obligation of inspectors and other employees of the Office for a concrete case.

C H A P T E R T W O

ACTIVITIES OF THE OFFICE

Section 38
Tasks of the Office

(1) The Office shall perform these tasks

a) continuous monitoring of the situation in personal data protection, information systems registration and keeping records on information systems,

b) recommending the controllers measures ensuring protection of personal data in information systems; for this purpose it issues recommendations for controllers in the scope of its competence,

c) in case of doubts whether the extent, content and manner of processing or use of processed personal data are in compliance with the purpose of their processing,

compatible with the purpose of processing or whether they are obsolete with respect to time and substance of this purpose the Office shall be issuing a binding opinion,

d) in case of doubts on transborder flow of personal data it is issuing binding opinion,

e) in case of doubts on the registration of the information system it is issuing a binding opinion,

f) receiving and handling complaints concerning violations of personal data protection,

g) summoning controller or operator to give explanation in case of suspicion of breaching of rules resulting from this act,

h) inspecting processing of personal data in information systems.

i) imposing sanctions when detecting violations of duties specified in this Act,

j) informing[31)] criminal justice agencies of suspicion of crime,

k) registering information systems and assuring access to registration situation,

l) participating in the drafting of generally binding regulations in the area of personal data protection,

m) issuing generally binding regulations in the scope of its competence,

n) presenting opinions on draft laws and drafts of other generally binding regulations that regulate processing of personal data,

o) submitting to the National Council of the Slovak Republic the report on the state of personal data protection at least once in two years.

(2) Tasks specified under paragraph 1 subparagraphs b) to e), j), l) to o) shall be the exclusive competence of the President of the Office.

(3) When the Office determines facts indicating that a law, other generally binding regulation or internal rules issued by the controller has violated fundamental rights and freedoms of natural persons in the course of processing their personal data the President of the Office may file a motion to have it amended or cancelled with the competent body.

I n s p e c t i o n a c t i v i t y

Section 39
Rights and duties of the inspection body

(1) The chief inspector and other inspectors (hereinafter the „controlling body“ as well as the President of the Office and Vice-president of the Office are entitled to

a) enter controller‘s and processor‘s premises, buildings or rooms of operations and facilities,

b) require that the controller, processor and their employees (hereinafter the „controlled person“) submit, within a given deadline, documents, other written materials, statements and information, data processed on memory media including technical data carriers, statements and software source codes, when they own these materials and also other materials needed for

31) Section 158 paragraph 1 Criminal Procedure Code.

inspection, originals and/or and in justified cases to enable taking of copies also outside the premises of the controlled person,

c) require full and true oral and written information, statements and explanations to inspected and related facts and linked deficiencies from the controlled person within a reasonable time limit,

d) require concurrence of the controlled person.

(2) The controlling body shall have the duty to

a) inform the controlled person of the matter of inspection in advance and to demonstrate their professional link with the Office,

b) draft an inspection report (hereinafter the „report"),

c) enter inspection findings in the report,

d) inform the controlled person of the inspection findings and ask from him/her written statements on all facts that justify calling for liability; to enter presented objections against the presented inspection findings with respect to their veracity, completeness and provability in the report,

e) give the controlled person one copy of the report or inspection statement or their copies,

f) confirm, in writing, the controlled person the receipt of copies of documents, written materials, memory media copies and other materials and to ensure their due protection against loss, damage or misuse.

(3) The inspection report shall include the name, seat or permanent residence of the controlled person, place and time of inspection, the person carrying out the inspection, established inspection findings, controlled person's statement to inspection findings, date of report drafting, name, functions and autographs of the inspection body and controlled person's responsible employees who were informed of the content of the report and the date of being informed of the report. When the controlled person refuses to be informed of the content of the inspection report, to make statements to inspection findings or to sign the inspection report this fact shall be stated in the inspection report.

(4) If the inspection establishes violation of duties stipulated herein the inspection body shall proceed subject to Section 46 in the imposition of measures removing the deficiencies identified by the inspection.

(5) If the inspection does not establish any violations of duties stipulated herein or in other laws[32)] the inspection body shall only draft an inspection statement. Its drafting shall follow the provisions of paragraph 3 as appropriate.

Section 40
The rights and duties of the controlled person

(1) At the time of being informed of inspection findings the controlled person shall be entitled to present objections against presented inspection findings with respect to their veracity, completeness and provability.

---

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

(2) The controlled person shall have the obligation to

a) create appropriate conditions for carrying out inspection and processing of inspection findings for the inspection body,

b) appropriately co-operate with the inspection body in compliance with the powers under Section 39 paragraph 1 and to abstain from conduct that could frustrate the inspection,

c) appear for acquainting himself/herself with the content of the report at the place specified by the inspection body within the specified time period,

d) sign the inspection report or statement after being informed of inspection findings; refusal to learn the content of the report or to sign the report by the controlled person shall be without prejudice to the consequences resulting from this document,

e) to submit, in writing, the inspection body measures adopted to remove the established shortcomings in specified intervals and a written report on the fulfilment of this measures.

Section 41
External resources

(1) When justified by the specific nature of the inspection task the inspection body can make use of other natural persons to carry out the inspection. The participation of these natural persons in the inspection shall be understood as another act in general interest. Provisions of Section 37 paragraph 6 and Section 39 paragraph 1 shall apply to external resources as appropriate.

(2) The inspection cannot be carried out by external resources who may give rise to doubts as to their prejudice due to their relation to the matter of inspection or to the controlled person. External resources who themselves know of facts giving rise of prejudice concerns shall inform the Office of these facts without any delay.

(3) The controlled person may present, in writing, provable prejudice objections with respect to external resources. Until the prejudice objection is decided external resources may perform only those acts that cannot be delayed while inspecting.

(4) The President of the Office shall decide on prejudice objection and information of bias. President's of the Office decision in this matter shall be final.

Section 42

(1) Other employees of the Office can be commissioned with a concrete task during inspection. Provisions of Section 39 paragraph 1 and 2 subparagraph a) shall apply to commissioned employees of the Office as appropriate.

(2) Inspectors and commissioned employees who themselves know of facts giving rise to bias concerns with respect to the matter of inspection or controlled person shall inform the President of the Office of these facts without any delay. When the President of the Office recognises bias he/she shall exclude the person concerned from acting in the matter.

Section 43

Regulations on inspection in state administration[33)] shall not apply to the performance of the inspection.

C o o p e r a t i o n

Section 44

(1) State administration authorities, bodies of territorial self-governments, other public authorities, controllers and processors shall provide the Office necessary assistance in the performance of its tasks (Section 38).

(2) The controller and processor shall give the office all data required by the Office during the performance of its tasks within the required time limit.

(3) When summoned the controller and processor shall appear before the Office to give explanation within the determined time limit.

(4) The controller and the processor shall be obliged to tolerate all acts by the Office aimed at examining all circumstances needed to assess the examined case objectively.

C H A P T E R T H R E E

REMEDIES

Section 45
Receiving and handling complaints

(1) Legal entities and natural persons may file, in writing, complaints concerning alleged violations of personal data protection [Section 38 paragraph 1 subparagraph f)]. A complaint filed by the controller or processor proper shall not be considered complaint.

(2) The Office shall examine and handle the complaint within 60 days from the date of receipt. The President of the Office may extend this term appropriately in justified cases, however, by not more than six months. The complainant must be informed of the term extension in writing.

(3) A special regulation[34)] with the exception of provisions of Sections 3 and 4, Sections 10 to 14, Section 18 and Section 21 shall apply to receiving and handling complaints concerning allegations of personal data protection violations as appropriate.

Section 46
Measure

(1) The Office

---

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

34) Act No. 152/1998 Coll. on complaints.

a) shall call the controller or processor to immediately block personal data or provisionally terminate the activity that could imperil the compliance with such obligation in case of allegations of violations of duties imposed herein,

b) shall issue a measure imposing termination of the activity that violated the duty, implementation of measures necessary to remove the deficiencies or secure rights and interests protected by law of data subjects with the specified period time when determining violation of duty laid down herein.

(2) The controller and processor shall immediately comply with the requirements of the Office under paragraph 1 and inform the Office of their fulfilment within the specified time limit.

(3) The controller and processor shall have the right to file, in writing, objection against the measure imposed pursuant to paragraph 1 subparagraph a) within three days from the day of its service. Objection against such measure shall have no suspensive effect.

(4) The controller and processor shall have the right to file, in writing, objection against the measure imposed pursuant to paragraph 1 subparagraph b) within seven days from the day of its service. Objection against such measure shall have suspensive effect.

(5) The President of the Office shall decide on the objection filed by the controller or processor under paragraph 3 within 15 days and on the objection filed under paragraph 4 within 60 days from the date of their receipt.

(6) President's of the Office decision on objections shall be final.

(7) Written calls to implement a measure and written decisions on objections are notified by delivery in one's own hands.

(8) The Office may cancel measures imposed under paragraph 1 subparagraph a); it shall lose effect on the day of notification of the measure in the matter under paragraph 1 subparagraph b).

Section 47

Provisions of Sections 45 and 46 shall be without prejudice to the right to judicial protection[35)]

Section 48

Disclosure of violations of law

When severe violations of data subjects' rights or other persons' freedoms occurred under this law the President of the Office may disclose the name, seat or permanent residence of the controller or processor and the description of the facts of the violation of personal data protection.

C H A P T E R F O U R

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

SANCTIONS FOR VIOLATING THE LAW

Section 49
Administrative wrongs

(1) The Office may impose a controller or processor a fine up to SKK 10,000,000 when they

a) process personal data in breach of Sections 5 to 7 and Section 10,

b) process special categories of personal data in breach of Section 8 or Section 9,

c) carry out processing with wrong or obsolete personal data (Section 12),

d) fail to liquidate wrong or obsolete data; liquidate or process personal data in breach of Section 13,

e) fail to comply with the notification obligation of correcting or liquidating personal data (Section 14),

f) fail to implement measures necessary for the protection of personal data against theft, loss, damage, unauthorised access, alteration or dissemination; fails to adopt measures in the form of security project or submits a security project that fails to include all particulars laid down herein (Section 15 paragraph 1 and 2 and section 16),

g) fail to arrange information system security audit or its drafting is in breach of this Act or fail to submit the evaluation report (Section 15 paragraphs 4 and 5),

h) fail to instruct legal entities and natural persons who have access to the information system (Section 17),

i) fail to comply with data subject's requirements or the obligation to give information to data subject (Section 20 and 21),

j) fail to notify of restricting data subject's rights (Section 22),

k) transfer personal data in breach of Section 23**,**

l) fail to give the Office requested data or explanations (Section 44 paragraphs 2 and 3), or

m) fail to comply with the requirements of the Office (Section 46 paragraphs 1 to 2).

(2) The Office may impose a controller who fails to comply with the registration obligation for an information system and with the linked duties resulting from this Act (Sections 25 to 28) a fine up to SKK 3,000,000.

(3) The Office may impose a controller who fails to comply with the record keeping obligation for an information system or who refuses the make data from records accessible (Sections 29, 30 and Section 32) a fine up to SKK 1,000,000.

(4) The Office may impose a controller who fails to commission, in writing, a responsible person with overseeing the personal data protection (Section 19 paragraph 2), fails to ensure his/her training or who cannot demonstrate that it was held (Section 19 paragraph 3) a fine up to SKK 500,000.

(5) The Office may impose a fine up to SKK 100,000 on those who

a) provide personal data in breach of Section 7 paragraph 5; this shall not apply to controllers and processors,

b) provides false personal data (Section 11),

c) breaches the confidentiality obligation with respect to personal data (Section 18) or

d) when the responsible person fails to inform the controller in writing (Section 19 paragraph 4).

(6) The Office may repeatedly impose fines under paragraphs 1 to 4 and Section 50 when the obligation was not satisfied within the specified term.

(7) When imposing fines mainly significance, duration and consequences of unlawful conduct shall be considered.

(8) The fine under paragraphs 1 to 5 may be imposed within one year from the day on which the Office determined the violation of the duty, however, not later than three years from the date of the commission of the violation of obligation.

(9) The Office may also impose the obliged the implementation of measures remedying the consequences of unlawful conduct within a specified period in its decision to fine.

(10) A remonstrance may be filed against the decision to fine within 15 days from its service. The President of the Office shall decide upon the remonstrance within 60 days from its receipt.

(11) The proceeds from fines shall be state budget income.

Section 50
Procedural fines

(1) The Office may impose a controller or processor a procedural fine

a) up to SKK 50,000 for failure to ensure appropriate conditions for the inspection [Section 40 paragraph 2 subparagraph a)],

b) up to SKK 500,000 when obstructing inspection [Section 40 paragraph 2 subparagraph b)]; when the controller or processor prove that inspection obstruction was caused by a responsible person his/her liability shall be limited and the responsible person shall become liable.

(2) The procedural fine may be imposed within one year from the date of the commission of the violation of obligation.

P A R T F O U R

COMMON, INTERIM AND FINAL PROVISIONS

Section 51
Common provision

(1) The general regulation concerning administrative procedure[36)] shall apply to proceedings under this act provided this act does not stipulate otherwise.

(2) The general regulation concerning administrative procedure shall not apply to

a) decisions concerning doubts under Section 6 paragraph 5, Section 23 paragraphs 7 and 10 and Section 25 paragraph 4,
b) assessment of data in information systems applying for registration (Section 27),
c) providing information to data subject (Sections 20 to 22),
d) decisions concerning prejudice objections and bias notifications (Section 41),
e) accepting and handling complaints (Section 45),
f) proceedings concerning measures (Section 46).

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

Section 52

(1) The controllers of already operational information systems shall bring these systems in compliance with this Act within six months from the effective day thereof, and, if required so hereunder, file them for registration within this period.

(2) Controllers who process personal data on the basis of a separate law that lacks provisions concerning particulars under Section 7 paragraphs 3, 5, 6 or under Section 9 paragraph 1 subparagraph a) may process personal data in the scope necessary to achieve the stipulated purpose without data subject's consent not later than 31 December 2003.

Section 53

(1) Obligations of state supervision authority overseeing personal data protection in information systems resulting from the existing regulations shall be transferred to the Office from the date of effect of this Act.

(2) The rights and duties resulting from labour relations between the Commissioner for personal data protection in information systems and the employees of the Personal Data Protection Inspection unit of the Office of the Government of the Slovak Republic shall fully be transferred to the Office from the date of effect of this Act.

(3) The property of the State under the administration of the Office of the Government of the Slovak Republic procured for the purpose of performing the function of state supervision of personal data protection in information systems shall be transferred under the administration of the Office from the date of effect of this Act.

(4) The Office of the Government of the Slovak Republic shall provide material and technical operation of the Office till 31 December 2002. The property of the State under the administration of the Statistical Bureau of the Slovak Republic procured for the purpose of registration of information systems containing personal data shall be transferred under the administration of the Office from the date of effect of this Act.

---

36) Act No. 71/1967 Coll. on administrative proceedings (Code of Administrative Rules).

(5) Obligations resulting for the Commissioner for personal data protection in information systems resulting from international personal data protection agreements shall be transferred to the Office from the date of effect of this Act.

Section 54

(1) The Commissioner for personal data protection in information systems appointed under the existing regulation shall become the President of the Office from the date of effect of this Act and he/she shall remain in this office till the end of the term he/she was appointed Commissioner for personal data protection in information systems.

(2) The President of the Office shall decide on the registration under this Act of information systems submitted for registration under the existing regulations within two months from the date of effect of this Act. When the President of the Office decides that such system shall not be subject to registration the Office shall notify the controller within the same time limit.

(3) Proceedings commenced before the effectiveness of this Act shall be completed pursuant to the existing regulations.

Section 55

Provisions of Section 23 paragraphs 1 to 7 shall not apply to transborder flow of personal data between the Slovak Republic and the European Union Member States from the date of accession of the Slovak Republic to the European Union.

F i n a l p r o v i s i o n s

Section 56
Transfer of rights

When the term Commissioner for personal data protection is used in legal provisions it shall be understood to mean President of the Office herein.

Section 57
Repealing provision

The following items are hereby repealed :

1. Act No. 52/1998 Coll. on the protection of personal data in information systems as amended by Act No. 241/2001 Coll.,

2. Decree of the Statistical Bureau of the Slovak Republic No. 155/1998 Coll. laying down details of the manner, form and procedure in registration of an information system containing personal data.

Section 58
Effect

This Act shall enter into effect on 1 September 2002 except Section 35 paragraph 2 that shall come into effect on 1 December 2003.

President of the Slovak Republic

Chairman of the National Council of the Slovak Republic

Prime Minister of the Government of the Slovak Republic