18

ACT

of 29 November 2017

on personal data protection and amending and supplementing certain Acts

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

Article I

CHAPTER ONE

FUNDAMENTAL PROVISIONS

Section 1
Subject Matter

This Act shall regulate:

a) protection of the rights of natural persons against unauthorised processing of their personal data;

b) rights, obligations, and responsibility during processing of personal data of natural persons;

c) status, activity and organisation of the Office for Personal Data Protection of the Slovak Republic (hereinafter as "Office").

Section 2

Personal data mean data relating to an identified or identifiable natural person who may be identified, directly or indirectly, particularly by reference to a general identifier, other identifier, such as name, surname, identification number, location data,[1]) or online identifier, or to one or more factors or features specific to the physical, physiological, genetic, psychological, mental, economic, cultural, or social identity of that natural person.

Section 3
Scope

(1) This Act applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form a part of a filing system or are intended to form a part of a filing system.

(2) Except section 2, section 5, Chapter Two and Chapter Three of the Act, this Act applies to the processing of personal data which are subject to the special regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.[2])

(3) This Act applies to the processing of personal data by the Police Force, Military Police, Corps of Prison and Court Guards, Financial Administration, Prosecutors Office, and Courts (hereinafter as "Competent Authority") for the purposes of preventing and detecting criminal activity, identifying criminal offenders, prosecuting criminal offences, or for the purposes of

enforcing decisions in a criminal proceeding including protection against threats to public order, and to prevent such threats (hereinafter as "performance of tasks for the purposes of criminal proceeding"); within the Chapter Two of this Act, the processing of personal data in accordance with the previous part of the sentence is only subject to the provisions laid down in section 52, section 59, section 67 and section 73.

(4) This Act applies to the processing of personal data:

a) in the context of the activities of a controller or processor with a headquarter, place of business, branch, establishment, or permanent residency located in the territory of Slovak Republic, regardless of whether the processing of personal data takes place in the Slovak Republic or not;

b) in the context of the activities of a controller or processor with a headquarter, place of business, branch, establishment, or permanent residency located outside of territory of the Slovak Republic, but in a place where Slovak Republic laws applies by virtue of public international law;

c) of the data subject who is in the Slovak Republic by controller or processor with a headquarter, place of business, branch, establishment, or permanent residency not located in a Member State, where the processing of personal data is related to

1. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subject in Slovak Republic; or

2. the monitoring of their behaviour as far as their behaviour takes place within Slovak Republic.

(5) This Act does not apply to the processing of personal data:

a) by a natural person in the course of a purely personal or household activity;

b) by the Slovak Information Service,[3]) by the Military Intelligence,[4])

c) by the National Security Authority for the purposes of performing security screenings and for the purposes of collecting documents on meeting the requirements of judicial competence for decision making for the Judicial Council of the Slovak Republic.[5])

Section 4

Free movement of personal data between the Slovak Republic and the Member States is guaranteed; the Slovak Republic shall not restrict or forbid transfer of personal data due to protection of fundamental rights of natural persons, particularly due to their right to privacy in connection with the processing of their personal data.

Section 5
Definitions

For the purposes of this Act:

a) consent of data subject means any serious and freely given, specific, informed and unambiguous indication of data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to such data subject;

b) genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

c) biometric data means personal data resulting from specific technical processing of personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

d) data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care data or services relating to health care provision, which reveal information about his or her health status;

e) processing of personal data means processing operation or set of processing operations which is performed on personal data or on sets of personal data, whether or not by automated means, particularly for collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure;

f) restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

g) profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects or features relating to a natural person, in particular to analyse or predict aspects or features concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

h) pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

i) log means a record concerning user's activity in an automated filing system;

j) encryption means transformation of personal data so that repeated processing shall only be possible after entering a selected parameter, such as the key or password;

k) online identifier means an identifier provided by an application, device, or protocol, in particular the IP address, cookies, log in data to online services, radio frequency identification tags which may leave traces which, in particular when combined with unique identifiers or other information, may be used to create profile of the data subject and identify him or her;

l) filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

m) personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

n) data subject means any natural person whose personal data is being processed;

o) controller means anyone, who alone or jointly with others, determines the purposes and means of the processing of personal data, and which processes personal data on its behalf; the controller or the specific criteria for its determination may be provided for in a special regulation or in an international treaty binding upon the Slovak Republic, if such regulation or treaty lays down the purpose and means of processing of personal data;

p) processor means anyone who processes personal data on behalf of the controller;

q) recipient means anyone, to whom the personal data are disclosed, whether a third party or not; however, public authorities which may receive personal data based on special regulation or international treaty binding upon the Slovak Republic in compliance with the applicable data protection rules to the relevant purposes of data processing shall not be regarded as recipients;

r) third party means anyone other than the data subject, controller, processor, or other natural person which, under the direct authority of the controller or processor, are authorised to process personal data;

s) data protection officer means a person appointed by controller or processor which fulfils the duties under this Act;

t) representative means a natural or legal person with a headquarter, place of business, branch, establishment, or permanent residency in a Member State designated by controller or processor in writing pursuant to section 35;

u) enterprise means a natural person - entrepreneur or legal person engaged in an economic activity, irrespective of its legal form, including partnerships of natural persons or associations of legal persons regularly engaged in an economic activity;

v) group of undertakings means a controlling undertaking and its controlled undertakings;

w) main establishment means:

1. as regards a controller with establishments in more than one Member State, the place of controller's central administration in the European Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the European Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

2. as regards a processor with establishments in more than one Member State, the place of its central administration in the European Union, or, if the processor has no central administration in the European Union, the establishment of the processor in the European Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Act;

x) corporate rules mean personal data protection policies which are adhered to by a controller or processor with a headquarter, place of business, branch, establishment, or permanent residency in the territory of Slovak Republic for purpose of transfers of personal data to a controller or processor in a third country;

y) code of conduct means a set of data subject's personal data protection policies which the controller or processor committed to adhere to;

z) international organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

aa) Member State is a state that is a member of the European Union or a contracting party to the Agreement on the European Economic Area;

ab) third country is a country other than a Member State;

ac) employee of the Office means an employee in an employment relationship or similar relationship pursuant to special regulation[6]) or a state employee who carries out civil service in a civil service employment relationship pursuant to special regulation.[7])

CHAPTER TWO

GENERAL RULES ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

TITLE ONE

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

Section 6
Principle of Lawfulness

Personal data shall be processed lawfully, and so to avoid infringement of the fundamental rights of the data subject.

Section 7
Principle of Purpose Limitation

Personal data shall be collected only for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with this purpose; further processing of personal data for archiving purpose, scientific or historical research purpose, or statistical purpose, if in compliance with special regulation[8]) and if appropriate safeguards of the protection of data subject's rights in accordance with section 78 paragraph 8, shall not be considered to be incompatible with the initial purpose.

Section 8
Principle of Data Minimisation

Personal data processed shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

Section 9
Principle of Accuracy

Personal data processed shall be accurate and, where necessary, kept up to date; reasonable and effective steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Section 10
Principle of Storage Limitation

Personal data shall be kept in a form which permits identification of data subject for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for

archiving purposes, scientific or historical research purposes or statistical purposes in accordance with special regulation[8]), and provided that appropriate safeguards of the protection of data subject's rights in accordance with section 78 paragraph 8 are adhered to.

Section 11
Principle of Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised, unlawful processing, against accidental loss, erasure or damage of personal data, using appropriate technical or organisational measures.

Section 12
Principle of Accountability

The controller shall be responsible for compliance with the fundamental principles of personal data processing, for compliance of personal data processing with the principles of personal data processing and shall be requested to demonstrate such compliance with the data processing principles at request.

Section 13
Lawfulness of Processing

(1) Processing of personal data shall be lawful only if is carried out based on at least one of the following legal bases:

a) the data subject has given consent to the processing of his or her personal data for at least one specific purpose;

b) processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing of personal data is necessary pursuant to a special regulation or international treaty binding upon the Slovak Republic;

d) processing of personal data is necessary in order to protect the life, health or property of the data subject or another natural person;

e) processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

f) processing of personal data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or rights of the data subject which require protection of personal data, in particular where the data subject is a child; this legal basis shall not apply to processing of personal data carried out by public authorities in the performance of their tasks.

(2) The legal basis for the processing of personal data in accordance with points c) and e) of paragraph 1 shall be laid down by this Act, special regulation, or in an international treaty binding upon the Slovak Republic; special law shall lay down the purpose of processing, the category of data subjects, and the list or scope of personal data processed. The personal data processed based on a special law may be disclosed, transmitted or made public from the filing system only if the special law lays down the purpose of disclosing or the purpose of publication, the list or scope of personal data processed which may be disclosed or made public, or the recipients to whom the personal data are disclosed.

(3) Where the processing of personal data for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a special regulation, the controller shall, in order to ascertain whether processing of personal data for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia

a) any link between the purpose for which the personal data have been collected and the purpose of the intended further processing of personal data;

b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to section 16, or whether personal data related to criminal convictions and offences are processed, pursuant to section 17;

d) the possible consequences of the intended further processing of personal data for data subject; and

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Section 14
Conditions for Consent to processing of personal data

(1) Where processing of personal data is based on data subject's consent, the controller is responsible at any time, to demonstrate that the data subject has consented to processing of his or her personal data.

(2) If the controller requires the data subject to consent to personal data processing, such consent must be distinguished from other matters and must be made in a clear and understandable and accessible form.

(3) The data subject shall have the right to withdraw, at any time, his or her consent to personal data processing involving the data subject. The withdrawal of consent shall not affect the lawfulness of personal data processing based on consent before its withdrawal; prior to giving consent, the data subject shall be informed thereof. The data subject can withdraw his or her consent as the same way as to give the consent.

(4) When assessing whether consent is freely given, account shall be taken in particular of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Section 15
Conditions Applicable for Consent in Relation to Information Society Services

(1) In relation to the offer of information society services[9]), the controller processes personal data based on a consent of the data subject lawfully where the data subject is at least 16 years old. Where the data subject is below the age of 16 years, such processing of personal data shall be lawful only if and to the extent that consent is given or authorised by a legal representative of that data subject.[10])

(2) The controller shall make reasonable efforts to verify that consent is given or authorised by the legal representative of the data subject in accordance with paragraph 1, taking into

consideration available technology.

Section 16
Processing of Special Categories of Personal Data

(1) The processing of special categories of personal data shall be prohibited. Special categories of personal data are data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

(2) The prohibition to process special categories of personal data shall not apply if:

a) the data subject has given explicit consent to the processing of those personal data for at least one specified purpose; the consent shall be considered to be invalid if it is excluded by a special regulation;

b) processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security, social protection law, or public health insurance in accordance with special regulation[11]), international treaty binding upon the Slovak Republic, or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the life, health, or property of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities by a civic association, foundation, or a not-for-profit body providing services of general utility, political party or movement, trade union organisation, recognised religious denomination or religious society, and on condition that the processing relates solely to their members or to those natural persons who have regular contact with them in connection with their purposes and that the personal data are not disclosed to the recipient without the written or otherwise reliably provable consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the exercise of a legal claim[12]) or whenever courts are acting in their judicial capacity;

g) processing is necessary based on public interest under this Act, special regulation, or international treaty binding upon the Slovak Republic, which are proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the data subject;

h) processing is necessary for preventive occupational medicine, provision of healthcare and services relating to the provision of healthcare, or for the purpose of public health insurance, where such data are processed by healthcare provider, health insurance company, person providing services relating to healthcare provision, or person conducting surveillance over healthcare and the qualified authorised person on its behalf who is bound by the confidentiality obligation with regard to the information he or she has learned during his or her activities, and by the obligation to adhere to the principles of professional ethics;

i) processing is necessary for social insurance, social security of policemen and soldiers, for provision of state social benefits, allowance in support of social integration of individual with

severe disability into society,[13]) provision of social services, taking the measures under social and legal protection of children and social guardianship, or for provision of help in poverty, or the processing is necessary for purpose to meet the obligations or enforce the rights of controller responsible for processing in the area of labour law and in the area of employment services, if the controller is requested to do so under special regulation[14]) or under international treaty binding upon the Slovak Republic;

j) processing is necessary due to public interest in the area of public health, such as the protection against serious cross-border threats to health or to safeguard high quality and safety of health care, drugs, dietetic foods, or medical devices based on this Act, special regulation, or international treaty binding upon the Slovak Republic laying down appropriate and specific measures to protect rights of the data subject, particularly the confidentiality obligation,[15])

k) processing is necessary for archiving purposes, scientific, historical research purposes, or statistical purposes under this Act, special regulation, or international treaty binding upon the Slovak Republic, which interests are appropriate with regard to the followed objective, respect the essence of the law protecting personal data, and lay down appropriate and specific measures to safeguard fundamental rights and interests of the data subject.

Section 17
Processing of personal data relating to criminal convictions or offence

Only a national authority may be the controller for the purposes of personal data processing in the register of convictions under special regulation[16]). Personal data relating to convictions of a crime or offence or relating to safety measures shall only be processed based on a special regulation or international treaty binding upon the Slovak Republic which provide for appropriate safeguards for the rights of the data subject.

Section 18
Processing of personal data which does not require identification

(1) If the purpose for which a controller processes personal data does or did require, the identification of a data subject by the controller, the controller shall not maintain, acquire or process additional information in order to identify the data subject for to the sole purpose of complying with this Act.

(2) Where, in cases defined in paragraph 1, controller is able to demonstrate that it is not in a position to identify the data subject, controller shall inform the data subject in an appropriate manner, if possible. In such cases, sections 21 to 26 shall not apply except where the data subject, for the purpose of his or her rights provides additional information enabling his or her identification.

TITLE TWO

RIGHTS OF THE DATA SUBJECT

FIRST PART

INFORMATION AND ACCESS TO PERSONAL DATA

Section 19
Information to be provided where personal data are collected from data subject

(1) Where personal data relating to a data subject are collected from the data subject, the controller is, at the time when personal data are obtained, obligated to provide the data subject

a) identifying information and contact details of the controller and, of controller's

representative, if he (or she) was designated;

b) contact details of data protection officer, if he (or she) was designated;

c) purpose of personal data processing for which the personal data are intended, as well as the legal basis for personal data processing;

d) legitimate interests pursued by the controller or by a third party, where the personal data are processed in accordance with point f) of section 13 paragraph 1;

e) identification of recipient or category of recipient, if any;

f) the fact that the controller intends to transfer personal data to a third country or international organisation, identification of the third country or international organisation, information about existence or absence of an adequacy decision by the European Commission (the hereinafter as "Commission"), or reference to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available, if the controller intends to transfer refer to in section 48 paragraph 2, section 49, or section 51 paragraphs 1 and 2.

(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c) right to withdraw the consent at any time;

d) right to lodge a complaint to initiate proceedings pursuant to section 100;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject shall provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, including profiling, referred to in section 22 paragraphs 1 and 4, in those cases, information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing of the personal data with information on that other purpose and any relevant further information as referred to in paragraph 2.

(4) Paragraphs 1 to 3 shall not apply to the extent to which the information was provided to the data subject prior to personal data processing.

Section 20
Information provided where personal data are not obtained from the data subject

(1) Where personal data have not been obtained from the data subject, the controller shall

provide the data subject with

a) identifying information and contact details of the controller and, of controller's representative, if he (or she) was designated;

b) contact details of data protection officer, if he (or she) was designated;

c) purpose of personal data processing for which the personal data are intended, as well as the legal basis for personal data processing;

d) the categories of personal data concerned,

e) identification of recipient or category of recipient, if any;

f) the fact that the controller intends to transfer personal data to a third country or international organisation, identification of the third country or international organisation, information about existence or absence of an adequacy decision by the Commission, or reference to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available, if the controller intends to transfer refer to in section 48 paragraph 2, section 49, or section 51 paragraphs 1 and 2.

(2) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following further information

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on point f) of section 13 paragraph 1, the legitimate interests pursued by the controller or by a third party;

c) the right to request from the controller access to and rectification, erasure of personal data, restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

d) right to withdraw the consent at any time;

e) the right to lodge a complaint to initiate proceedings pursuant to section 100,

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, referred to in section 22 paragraphs 1 and 4 and, at least in those cases, information about the logic involved, as well as the significance of automated decision-making and the envisaged consequences of such processing for the data subject.

(3) The controller shall provide the information referred to in paragraphs 1 and 2

a) at least within one month after obtaining the personal data, having regard to the specific circumstances in which the personal data are processed,

b) at least at the time of the first communication to that data subject, if the personal data are to be used for communication with the data subject,

c) at least when the personal data are first disclosed, if a disclosure to another recipient is envisaged.

(4) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing of personal data with information on that other purpose and any relevant further information as referred to in paragraph 2.

(5) Paragraphs 1 to 4 shall not apply where:

a) in so far as the data subject already has the information;

b) in so far as the provision of such information proves impossible or would involve a disproportionate effort, in particular for personal data processing for archiving purposes, scientific purpose, historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in section 78 paragraph 8 or in so far as the obligation referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that personal data processing; in such cases the controller shall take appropriate measures to protect the data subject's rights and legitimate interests of data subject, including making the information publicly available;

c) in so far as obtaining or disclosuring of such information is laid down in a special regulation to which the controller is subject and which provides appropriate measures to protect the data subject's rights and legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of confidentiality pursuant to special regulation.[15])

Section 21
Right of Access to Personal Data

(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. Where the controller processes such personal data, the data subject has right of access to the personal data and the following information:

a) the purposes of the personal data processing;

b) the categories of personal data concerned;

c) identification of the recipient or category of recipient to whom the personal data have been or will be disclosed, in particular recipient in third country or international organisations, where possible;

d) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

e) the right to request the controller to rectify personal data regarding the data subject or their erasure or restriction or the right to object to processing of the personal data;

f) the right to lodge a complaint to initiate proceedings pursuant to section 100;

g) source of personal data, where the personal data are not collected from the data subject;

h) the existence of automated decision-making, including profiling, referred to in section 28 paragraphs 1 and 4 and, at least in those cases, controller shall provide information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where the personal data are transferred to a third country or international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to section 48 paragraphs 2 to 4 relating to the transfer.

(3) The controller shall provide the data subject his or her personal data undergoing processing. For any further providing of personal data requested by the data subject, the controller may charge a reasonable fee based on administrative costs. The controller shall provide personal data to the data subject in a form as requested by the data subject.

(4) The right to obtain personal data pursuant to paragraph 3 shall not adversely affect the rights of others.

SECOND PART

RECTIFICATION AND ERASURE AND RESTRICTION OF PERSONAL DATA PROCESSING

Section 22
Right to rectification of personal data

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed.

Section 23
Right to erasure of personal data

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

(2) The controller shall have the obligation to erase personal data without undue delay where the data subject exercised the right to erasure pursuant to paragraph 1 where:

a) the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point a) of section 13 paragraph 1 or point a) of section 16 paragraph 2, and where there is no other legal ground for the personal data processing;

c) the data subject objects to the processing of personal data pursuant to section 27 paragraph 1 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to section 27 paragraph 2;

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with this Act, or a special regulation or international treaty which is binding upon the Slovak Republic, or

f) the personal data have been collected in relation to the offer of information society services referred to in section 15 paragraph 1.

(3) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers which are processing the personal data that the data subject has

requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(4) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation under this Act, special regulation or international treaty binding upon the Slovak Republic or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with point h) to point j) of section 16 paragraph 2;

d) for archiving purpose, scientific purpose, historical research purpose or statistical purposes in accordance with section 78 paragraph 8 in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the exercise of a legal claim.

Section 24
Right to restriction of personal data processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b) the processing of personal data is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the exercise of legal claim;

d) the data subject objects to personal data processing pursuant to section 27 paragraph 1 pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing of personal data has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the purpose of exercising legal claim or for the protecting of the rights of other persons or for reasons of important public interest.

(3) A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Section 25
Notification obligation regarding rectification, erasure or restriction of personal data processing

(1) The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with section 22, section 23 paragraph 1 or section 24 to the recipient, unless this proves impossible or involves disproportionate effort.

(2) The controller shall inform the data subject about recipients pursuant to paragraph 1 if the data subject requests it.

THIRD PART

RIGHT TO PORTABILITY, RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

Section 26
Right to personal data portability

(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, if technically feasible, where:

a) the processing of personal data is based on point a) of section 13 paragraph 1, point a) of section 16 paragraph 2, or point b) of section 13 paragraph 1; and

b) the processing of personal data is carried out by automated means.

(2) The exercise of the right referred to in paragraph 1 shall be without prejudice to section 23. The right to portability shall not apply to processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(3) The right referred to paragraph 1 shall not adversely affect the rights of others.

Section 27
Right to object to personal data processing

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her which is based on points e) or f) of section 13 paragraph 1, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the rights or interests of the data subject or for the exercise of a legal claim.

(2) The data subject shall have the right to object to processing of personal data concerning him or her for the purposes of direct marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing of personal data for direct marketing purposes, the personal data shall no longer be processed by the controller for such purposes.

(3) The controller shall at the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 explicitly brought to the attention of the data subject and information about these rights shall be presented clearly and separately from any other information.

(4) In the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.

(5) Where personal data are processed necessary for the performance of a task carried out in the public interest, where personal data are processed for scientific purpose, historical research purposes or statistical purposes pursuant to section 78 paragraph 8, the data subject, on grounds relating to his or her particular situation, shall have the right to object to

processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Section 28
Automated individual decision-making, including profiling

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is made based on a special regulation or international treaty binding upon the Slovak Republic and which also lay down suitable measures to safeguard the data subject's rights and legitimate interests; or

c) is based on the data subject's explicit consent.

(3) In the cases referred to in points a) and c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and legitimate interests, in particular the right to verification of the decision in other than the automated manner by the controller, to express his or her point of view and to contest the decision.

(4) Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in section 16 paragraph 1, unless points a) or g) of section 16 paragraph 2 applies and suitable measures to safeguard the data subject's rights and legitimate interests are in place.

FOURTH PART

OBLIGATIONS OF CONTROLLER IN EXERCISE OF DATA SUBJECT´S RIGHTS

Section 29

(1) The controller shall implement appropriate measures and provide information for data subject referred to in sections 19 and 20 and any communication under sections 21 to 28 and section 41 relating to processing of personal data to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in a documentary form or in the electronic form, usually using the form used to file the application. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

(2) The controller shall provide cooperation to the data subject in the exercise of his or her rights pursuant to sections 21 to 28. In the cases referred to in section 18 paragraph 2, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under sections 21 to 28, unless the controller demonstrates that it is not in a position to identify the data subject.

(3) The controller shall provide information on action taken on a request under sections 21 to 28 to the data subject within one month of receipt of the request. That period may be extended by two further months, and even repeatedly, in justified cases, taking into account the complexity and number of the requests. The controller shall inform the data subject of any

such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the controller shall provide information by electronic means, unless otherwise requested by the data subject.

(4) If the controller does not take action on the request of the data subject, the controller shall inform the data subject within one month of receipt of the request of the reasons for not taking action and on the possibility to submit a complaint with the Office refer to in section 100.

(5) Information provided under sections 19 and 20 and any communication and any actions taken under sections 21 to 28 and section 41 shall be provided free of charge. Where request from a data subject is manifestly unfounded or excessive, in particular because of its repetitive character, the controller may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

b) refuse to act on the request.

(6) The controller shall prove that the request has manifestly unfounded or excessive character.

(7) Without prejudice to section 18, where the controller has reasonable doubts concerning the identity of the data subject submitting the request referred to in sections 21 to 27, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(8) The information to be provided to data subject pursuant to sections 19 and 20 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing of personal data. Where the icons are presented electronically they shall be machine-readable.

(9) The information to be presented by standardised icons and the procedures for providing standardised icons shall be determined in a legislative act of general application to be issued by the Office.

FIFTH PART

RESTRICTIONS

Section 30
Restrictions of Data Subject's Rights

(1) Controller or processor may, under the terms and conditions laid down by a special regulation or international treaty binding upon the Slovak Republic, restrict the scope of obligations and rights in accordance with sections 19 to 29 and pursuant to section 41, as well as the principles pursuant to sections 6 to 12, where relating to the rights and obligations under sections 19 to 29, when such restriction is laid down in order to safeguard:

a) security of the Slovak Republic;

b) defence of the Slovak Republic;

c) public order;

d) performance of tasks for the purposes of a criminal proceeding;

e) other important objectives of general public interest of the European Union or of the Slovak Republic, in particular an important economic or financial interest of the European Union or of the Slovak Republic, including monetary, budgetary and taxation a matters, public health and social security;

f) the protection of judicial independence and judicial proceedings;

g) the prevention of breaches of ethics for regulated professions or regulated professional activities;

h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points a) to e) and g);

i) the protection of the rights of the data subject or of others;

e) the exercise of a legal claim;

k) economic mobilisation.

(2) The controller or the processor may only take action pursuant to paragraph 1 where special regulation or an international treaty binding upon the Slovak Republic lays down at least

a) the purpose of the processing of personal data or categories of processing of personal data,

b) the category of personal data;

c) the scope of restriction introduced;

d) the safeguards to prevent abuse or unlawful access or transfer of personal data,

e) the specification of the controller or categories of controllers,

f) the storage periods and the applicable safeguards taking into account the nature, scope and purpose of the processing or categories of processing of personal data,

g) the risks to the rights of the data subject and

h) the right of data subject to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

TITLE THREE

RIGHTS AND OBLIGATIONS OF CONTROLLER AND PROCESSOR

FIRST PART

GENERAL OBLIGATIONS OF CONTROLLER AND PROCESSOR

Section 31
Controller

(1) Taking into account the nature, scope and purpose of processing as well as the risks of varying likelihood and severity for the rights of a natural person, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act. Those measures shall be updated where necessary.

(2) Where proportionate in relation to processing activities, the measures referred to in

paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

(3) Adherence to approved codes of conduct as referred to in section 85 or approved certification mechanisms as referred to in section 86 may be used as an element by which to demonstrate compliance with the obligations of the controller referred to in paragraph 1.

(4) The controller shall regularly review continued existence of the purpose of processing of personal data and, once fulfilled, take care of erasure without any undue delay; this shall not apply where the personal data form a part of registry records.[17])

(5) The controller shall take care of discarding of a registry record which contains personal data in compliance with the special regulation.[18])

Section 32
Data protection by design and by default

(1) The controller shall, prior to processing of personal data implement and at the time of the processing itself have implemented data protection by design consisting of appropriate technical and organisational measures, in particular pseudonymisation, for efficient implementation of appropriate safeguards of data protection and adhere to the fundamental principles referred to in sections 6 to 12.

(2) In the case of data protection by design, the controller shall take into account the state of the art, the cost of implementation referred to in paragraph 1, the nature, scope, context and purposes of processing and risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

(3) The controller shall implement personal data protection by default consisting of implementation of appropriate technical and organisational measures to ensure that processing of personal data only for specific purpose, minimise the amount of personal data collected and the scope of their processing, period of storage, and accessibility of personal data. The controller shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(4) A certificate pursuant to section 86 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 to 3.

Section 33
Joint Controllers

(1) Where two or more controllers jointly by arrangement determine the purposes and means of processing, they shall be joint controllers. In arrangement, they shall in a transparent manner determine their respective responsibilities for compliance with the obligations and tasks under this Act, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in sections 19 and 20, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by special regulation or an international treaty binding upon the Slovak Republic. The arrangement shall designate a contact point for data subject.

(2) The essence of the arrangement referred to in paragraph 1 shall be made available to the data subject; in particular, identification of the parties to the arrangement, subject-matter, term of the arrangement, provisions regulating the exercise of rights of the data subject, obligations of controllers to provide information pursuant to sections 19 and 20 and the contact point for the data subject.

(3) Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights in respect of and against each of the controllers.

Section 34
Processor

(1) Where processing is to be carried out on behalf of a controller, the controller may authorise only processor providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Act and ensure the protection of the rights of the data subject. The consent of data subject shall not be required for the authorisation of processor for processing of personal data pursuant to the first sentence.

(2) The processor shall not engage another processor without prior specific written consent or general written authorisation of the controller for processing of personal data. In the case of general written authorisation, the processor shall inform the controller in advance of authorising another processor.

(3) Processing of personal data by a processor shall be governed by a contract or other legal act that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the list or scope of personal data, the categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor shall:

a) process the personal data only on written instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless transfer by a special regulation or international treaty binding upon the Slovak Republic; in such transfer, the processor shall inform the controller of that legal requirement before processing the personal data, unless a special regulation or treaty biding upon Slovak Republic prohibits such information on grounds of public interest;

b) ensure that persons authorised to process the personal data have committed themselves to confidentiality unless they are bound by confidentiality pursuant to special law[15]);

c) take all measures pursuant to section 39;

d) respect the conditions referred to in paragraphs 2 and 5 for engaging another processor;

e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to take action at the request of the data subject under the Title two of Chapter two;

f) assist the controller in ensuring compliance with the obligations pursuant to sections 39 to 43 taking into account the nature of processing and the information available to the processor;

g) delete personal data or return the personal data to the controller after the end of the provision of services relating to processing of personal data based on controller's decision, and delete existing copies which contain personal data, unless special regulation or international treaty binding upon the Slovak Republic requires storage of that personal data;

h) at the choice of the controller, delete or return the personal data to the controller after the end of the provision of services relating to processing of personal data, and delete existing copies which contain personal data, unless special regulation or international treaty binding

upon the Slovak Republic requires storage of that personal data;

i) make available to the controller information necessary to demonstrate compliance with the obligations and provide cooperation within personal data protection audit and inspection executed by the controller or another auditor mandated by the controller.

(4) The processor shall immediately inform the controller if, in its opinion, an instruction given by controller infringes this Act or special regulation or international treaty binding upon the Slovak Republic concerning personal data protection.

(5) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Act. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(6) Processor may demonstrate sufficient guarantees as referred to in paragraphs 1 and 5 by way of an approved code of conduct refer to in section 85 or a certificate refer to in section 86.

(7) The contract or other legal act referred to in paragraphs 3 and 5 shall be entered into in a documentary or electronic form.

(8) Without prejudice to sections 38 and sections 104 to 106, processor which infringed this Act by determining the purposes and means of processing of personal data, shall be considered to be a controller in respect of that processing.

Section 35
Representative of Controller or Representative of Processor

(1) The controller or the processor which do not have a headquarter, branch, establishment or permanent residency in a Member State shall designate in writing a representative in the Member State, where that controller or processor processes personal data of a data subject resident to the Slovak Republic, provided that the processing activity relates to

a) the offering of goods or services to such data subject irrespective whether or not a payment is requested from the data subject in the territory of the Slovak Republic; or

b) the monitoring of their behaviour in the territory of the Slovak Republic.

(2) The obligation laid down in paragraph 1 shall not apply to:

a) processing of personal data which is occasional, does not include, on a large scale, processing of special categories of data as referred to in section 16 paragraph 1 or processing of personal data relating to criminal convictions and offences referred to in section 17, and is unlikely to result in a risk to the rights of natural persons, taking into account the nature, context, scope and purpose of the processing; or

b) a public authority or public institution.

(3) The office and the data subject may request information relating to the processing of personal data to safeguard compliance with this Act by controller and processor, as well as

by the representative of controller or the representative of the processor.

(4) The designation of a representative by the controller or processor shall be without prejudice to the rights of the data subject to lodge a complaint in accordance with section 100 or to any other legal protection under special regulation[19]) that may be enforced against controller or processor.

Section 36
Processing of personal data under the surveillance of the controller or processor

The processor and any person acting on behalf of the controller or the processor who has access to personal data shall only process those personal data on instruction from the controller or pursuant to a special regulation or international treaty binding upon the Slovak Republic.

Section 37
Records of processing activities

(1) The controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. The record shall contain:

a) identifying information and contact details of the controller, joint controller, controller's representative, where applicable, and data protection officer;

b) the purpose of personal data processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients including recipient in third country or international organisation;

e) where controller indents to transfer personal data to a third country or an international organisation, the identification of that third country or international organisation and, where the controller intends to transfer the data pursuant to section 51 paragraphs 1 and 2, and the documentation of suitable safeguards;

f) the envisaged time limits for erasure of the different categories of data;

g) a general description of the technical and organisational security measures referred to in section 39 paragraph 1.

(2) The processor and, where applicable, the processor's representative, shall maintain a record of the categories of processing activities carried out on behalf of the controller. Such record shall contain:

a) identifying information and contact details of the processor and the controller, on behalf of which the processor is acting, the representative of the controller or processor, where applicable, and the data protection officer;

b) the categories of processing of personal data carried out on behalf of each controller;

c) where controller indents to transfer personal data to a third country or an international organisation, and, where the controller intends to transfer the data pursuant to section 51 paragraphs 1 and 2, the documentation of suitable safeguards;

d) a general description of the technical and organisational security measures referred to in section 39 paragraph 1.

(3) The records referred to in paragraphs 1 and 2 shall be kept in a written or electronic form.

(4) The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record of processing activities available to the office on request.

(5) The obligations referred to in paragraphs 1 and 2 shall not apply to an employer with fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights of the data subject, the processing is not occasional, or the processing includes special categories of data as referred to in section 16 paragraph 1 or personal data relating to criminal convictions and offences referred to in section 17.

(6) The template of the record of processing activities shall be published by the office on its website.

Section 38
Right to compensation and liability

(1) Any person who has suffered material or non-material damage as a result of an infringement of this Act shall have the right to receive compensation[20]) from the controller or processor for the damage suffered.

(2) The controller involved in processing of personal data shall be liable for the damage caused by unlawful processing. A processor shall be liable for the damage caused by processing of personal data only where it has not complied with obligations under sections 34 to 37, section 39, section 40 paragraph 3, section 44, section 45, section 51 paragraph 3 or where it has acted outside or contrary to instructions of the controller which were in line with the Act.

(3) A controller or processor may be exempt from liability under paragraph 2 if it proves that it is not responsible for the event giving rise to the damage.

(4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing of personal data and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, they shall be jointly and severally held liable for the damage.

(5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

SECOND PART

SECURITY OF PERSONAL DATA

Section 39
Security of processing

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of processing as well as the risk of varying likelihood and severity for the rights of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk,

including particularly:

a) the pseudonymisation and encryption of personal data;

b) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems;

c) the process of restoration of the availability and access to personal data in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the personal data processing.

(2) In assessing the appropriate level of security account shall be taken of the risks that are presented by processing of personal data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3) Adherence to an approved code of conduct as referred to in section 85 or a certificate as referred to in section 86 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.

(4) The controller and processor shall ensure that natural person acting under on behalf of the controller or the processor who has access to personal data only process them based on instructions from the controller, or based on a special regulation or international treaty binding upon the Slovak Republic.

Section 40
Notification of a personal data breach to the Office

(1) Controller shall notify the personal data breach to the Office no later than 72 hours after having become aware of it; this shall not apply if the personal data breach is unlikely to result in a risk to the rights of a natural person.

(2) Where the controller fails to meet the notification duty as referred to in paragraph 1, the controller shall provide reasoning of such failure.

(3) The processor shall notify personal data breach the controller without any undue delay after becoming aware of it.

(4) The notification referred to in paragraph 1 shall particularly contain:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) The controller shall provide the information referred in paragraph 4 to the extent to which such information is known to the controller at the time of notification pursuant to paragraph 1; if the controller does not have all information referred to in paragraph 4 at the time of notification pursuant to paragraph 1, the controller shall provide them as soon as he becomes aware of it.

(6) The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Section 41
Communication of a personal data breach to the data subject

(1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain the information and measures referred to in points b) to d) of section 40 paragraph 4.

(3) The communication referred to in paragraph 1 shall not be required if:

a) the controller has implemented appropriate technical and organisational protection measures, and they were applied to the personal data affected by the personal data breach, in particular encryption and other measures that render the personal data unintelligible to any person who is not authorised to access it,

b) the controller has taken subsequent measures to safeguard the high risk to the rights of data subjects referred to in paragraph 1;

c) it would involve disproportionate effort; controller shall inform the public or take other measures whereby the data subject is informed in an equally effective manner.

(4) If the controller has not already communicated the personal data breach to the data subject, the Office, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

THIRD PART

DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Section 42
Data protection impact assessment

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the personal data processing, may result in a high risk to the rights of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment is sufficient to address a set of similar processing operations that present similar high risks.

(2) The controller shall consult each procedures wit data protection officer, where designated, when carrying out a data protection impact assessment.

(3) A data protection impact assessment shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects or features relating to the data subject which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the data subject or similarly significantly affect the data subject;

b) processing on a large scale of special categories of personal data refer to in section 16 paragraph 1 or personal data relating to criminal convictions and offences refer to in section 17; or

c) a systematic monitoring of a publicly accessible area on a large scale.

(4) A data protection impact assessment shall in particular contain:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights of the data subject; and

d) the measures to elimination of the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act taking into account the rights and legitimate interests of data subjects and other natural persons concerned.

(5) Compliance with approved codes of conduct referred to in section 85 or the certificate referred to in section 86 by the controller or processor shall be taken into due account in assessing the impact of the processing operations performed by such controller or processor, in particular for the purposes of a data protection impact assessment.

(6) The controller may seek the views of the data subject or the organisation that represents his or her interests on the intended processing of personal data, without prejudice to the protection of commercial or public interests or the security of processing operations.

(7) The controller shall assess if processing is performed in accordance with the data protection impact assessment, particularly when there is a change of the risk represented by processing operations.

Section 43
Prior consultation

(1) The controller shall consult the Office prior to processing of personal data where a data protection impact assessment under section 42 indicates that the processing of personal data would result in a high risk for rights of natural person in the absence of measures taken by the controller to mitigate the risk.

(2) Where the Office is of the opinion that the intended processing referred to in paragraph 1 would infringe this Act, in particular where the controller has insufficiently identified or mitigated the risk, the Office shall, within the period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller or to the processor. The Office may, considering the complexity of intended processing of personal data, extend the time period set forth in the previous sentence by six weeks; the Office shall notify the

controller or the processor about the extension and its justification within one month of receiving the request for consultation by written form. The period for consultation is suspended until the Office collects the information requested for the purposes of consultation.

(3) When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the Office with:

a) information about the obligations of the controller which the controller has in connection with its processing activity subject to previous consultation pursuant to paragraph 1, about the joint controllers and processors involved in the processing of personal data, in particular for processing the personal data within a group of undertakings;

b) information about the purposes and means of the intended processing of personal data;

c) information about the measures and safeguards provided to protect the rights of the data subject pursuant to this Act;

d) where applicable. contact details of data protection officer;

e) the data protection impact assessment referred to in section 42; and

f) other information requested by the Office.

FOURTH PART

DATA PROTECTION OFFICER

Section 44
Designation of the data protection officer

(1) The controller and the processor shall designate a data protection officer where:

a) the processing of personal data is carried out by a public authority or public institution, except for courts acting in their judicial capacity;

b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subject on a large scale; or

c) the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data refer to in section 16 or personal data relating to criminal convictions and offences on a large scale refer to in section 17.

(2) A group of undertakings may appoint a single data protection officer provided that a data protection officer is qualified to fulfil the tasks referred to in section 46 for each enterprise from the group of undertakings.

(3) Where the controller or the processor is a public authority or public institution, a single data protection officer may be designated for several such authorities or institutions, taking account of their size and organisational structure.

(4) In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

(5) In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors shall designate a data protection officer, where so requested under special regulation or international treaty binding upon the Slovak Republic. The data protection officer may act for such associations and other bodies representing the controllers or processors.

(6) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in section 46.

(7) The data protection officer may be an employee of the controller or processor, or fulfil the tasks on the basis of a contract.

(8) The controller and the processor shall publish, e.g. on its web site, the contact details of the data protection officer, where appropriate, and communicate them to the Office.

Section 45
Position of the data protection officer

(1) The controller and the processor shall ensure that the data protection officer carries out, properly and in a timely manner, all activities which relate to the protection of personal data.

(2) The controller and processor shall provide cooperation to the data protection officer in performing the tasks referred to in section 46 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of the tasks referred to in section 46. He or she shall not be dismissed or penalised by the controller or the processor for performing the tasks refer to in section 46. The data protection officer shall directly report to the statutory body of the controller or the processor during fulfilment of the tasks under section 46.

(4) Data subject may contact the data protection officer with regard to issues related to processing of their personal data and to the exercise of their rights under this Act.

(5) The data protection officer shall be bound by confidentiality concerning the performance of his or her tasks, in accordance with this Act or special regulation.[15])

(6) The data protection officer may also fulfil other tasks and duties than refer to in section 46; the controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Section 46
Tasks of the data protection officer

(1) The data protection officer shall, in particular:

a) provide information and advise the controller or the processor and the employees who carry out processing of personal data of their obligations in accordance with this Act, special regulations, or international treaties binding upon the Slovak Republic concerning the data protection provisions;

b) monitor compliance with this Act, special regulations, or international treaties binding upon the Slovak Republic concerning the data protection provisions and with the policies of

the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of persons involved in processing operations, and the related audits of personal data protection,

c) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 42,

d) cooperate with the Office during performance of his or her tasks;

e) act as the contact point for the Office on issues relating to processing, including the prior consultation referred to in section 43, and consult, where appropriate, with regard to other matter.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of personal data processing.

TITLE FOUR

TRANSFER OF PERSONAL DATA TO THIRD COUNTRY OR INTERNATIONAL ORGANISATION

Section 47
General principle of transfer

Transfer of personal data which is undergoing processing or is intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions are complied with by the controller and processor, including conditions for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

Section 48
Transfer of personal data to third country or to international organisation

(1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of personal data protection. Such a transfer shall not require any specific authorisation.

(2) In the absence of a decision by the Commission referred to in paragraph 1, the personal data may only be transferred to a third country or an international organisation if appropriate safeguards to protect personal data are provided.

(3) The appropriate safeguards referred to in paragraph 2 may be provided, for without requiring any specific authorisation from the Office, by:

a) an international treaty binding upon the Slovak Republic,

b) corporate rules in accordance with section 49,

c) standard data protection clause adopted by the Commission,

d) standard data protection clause adopted by the Office,

e) an approved code of conduct pursuant to section 85 together with commitments of the

controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights, or

f) a certificate pursuant to section 86 together with commitment of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

(4) The appropriate safeguards referred to in paragraph 2 may also be provided for with requiring authorisation from the Office, in particular, by:

a) contractual clauses between the controller or processor and the controller, processor or the recipient in the third country or international organisation, or

b) provisions into administrative arrangements between public authorities or public institutions which include effective means to enforce data subject rights to lodge a complaint pursuant to section 100 and to other legal protection in accordance with a special regulation.[19])

Section 49
Corporate Rules

(1) The Office shall approve corporate rules, if

(a) apply to and are enforced by every member of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

b) expressly regulate internal procedures for exercise of the rights on the data subject, where personal data processing is concerned; and

c) fulfil the requirements laid down in paragraph 2.

(2) The corporate rules shall specify at least:

a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members,

b) the data transfer or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects and the identification of the third country or countries,

c) their binding nature, for the controller and for the processor;

d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security of personal data, and the requirements in respect of onward transfers to bodies not bound by the corporate rules,

e) the rights of the data subject in regard to processing of personal data and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with section 28, the right to lodge a complaint pursuant to section 100 and to other legal protection of right pursuant to a special regulation[19]) and the right to compensation for a breach of the corporate rules,

f) the acceptance by the controller or processor with a headquarter, branch, establishment, or

permanent residency on the territory of the Slovak Republic of liability for any breaches of the corporate rules by any member concerned not having a headquarter, branch, establishment, or permanent residency in any Member State; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that controller or processor is not responsible for the damage,

g) how the information about the corporate rules, in particular on the provisions referred to in points d) to f) of this paragraph is provided to the data subject in addition to sections 19 and 20,

h) the task of data protection officer or other person or entity in charge of the monitoring compliance with the corporate rules, as well as monitoring training and complaint-handling,

i) the complaint initiation procedure,

j) the mechanism within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the corporate rules which includes data protection audits and methods for ensuring corrective actions to protect the rights of the data subject; results of such verification should be communicated to the data protection officer or entity referred to in point h) and to the statutory body of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the Office,

k) the mechanism for reporting and recording changes to the rules and reporting those changes to the Office,

l) the cooperation mechanism with the Office to ensure compliance with the rules, in particular by making available to the Office the results of verifications referred to in point j),

m) the mechanism for reporting a legal requirement to which the controller or processor is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the corporate rules; and

n) the appropriate data protection training to natural persons having permanent or regular access to personal data.

Section 50

Transfers or disclosures of personal data not authorised by the Slovak Republic law

The judgement of a court, or tribunal and decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable if based on an international agreement concluded with the third country which is binding upon the Slovak Republic or the European Union.

Section 51

Derogations for specific situations

(1) In the absence of an adequacy decision pursuant to section 48 paragraph 1 or of appropriate safeguards pursuant to section 48 paragraphs 2 to 4, including corporate rules, a transfer of personal data to a third country or an international organisation shall take place only where:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards,

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request,

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person,

d) the transfer is necessary based on public interest pursuant to a special regulation or international treaty binding upon the Slovak Republic,

e) the transfer is necessary for the exercise of a legal claim of the data subject,

f) the transfer is necessary in order to protect the life, health or property of the data subject or of other natural person, where the data subject is physically or legally incapable of giving consent, or

g) the transfer is made from a register which according to special regulation or international treaty binding upon the Slovak Republic is intended to provide information to the public and which is open to consultation by the public, but only to the extent that the conditions laid down under this Act, special regulation, or international treaty binding upon the Slovak Republic for consultation are fulfilled.

(2) Where a transfer cannot be carried out in accordance with section 48 and none of the derogations for a specific situation referred to in paragraph 1 is applicable, the transfer of personal data to a third country or international organisation may only take place if:

a) the transfer is not of a repetitive nature,

b) the transfer only concerns to a limited number of data subject,

c) the transfer is necessary for the purpose of compelling legitimate interests pursued by the controller which are not overridden by the rights or legitimate interests of the data subject, and

d) the controller has assessed the circumstances surrounding the data transfer and has provided suitable safeguards with regard to the protection of personal data.

(3) The controller is obliged to inform the Office of the transfer as referred in paragraph 2 in advance. The controller is obliged to, in addition to providing the information referred to in sections 19 and 20, inform the data subject of the transfer as referred in paragraph 2 and of its legitimate interests within time periods pursuant to section 37. The controller and the processor shall provide for documentation of the assessment as well as appropriate safeguards in records of processing activities as referred in section 37.

(4) A transfer pursuant to point g) of paragraph 1 shall not involve personal data or entire categories of personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

(5) Points a) to c) of paragraph 1 and paragraph 2 do not apply to activities carried out by public authorities in the exercise of their public powers.

CHAPTER THREE

SPECIAL RULES ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES

TITLE ONE

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

Section 52

Procedures of competent authorities with regard to processing personal data for performance of tasks for the purposes of criminal proceeding are governed by section 6, section 8, section 9, section 11, section 12 and section 13 paragraph 2 equally.

Section 53
Principle of purpose limitation

Personal data shall be collected for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with this purpose; the same competent authority or another competent authority is authorised to process personal data for archiving, scientific purpose or historical research purpose or statistical purpose with regard to completing tasks related to criminal proceedings, where implement appropriate safeguard to protect rights of data subject.

Section 54
Principle of storage limitation

Personal data shall be kept in a form which permit identification of the data subject for no longer than is necessary for the purpose for which the personal data are processed.

Section 55
Principle of lawfulness of processing

(1) The competent authority may process personal data for performance of tasks for the purposes of criminal proceeding pursuant to this Act, the special regulation or an international treaty binding upon the Slovak Republic.

(2) Processing of personal data for performance of tasks for the purposes of criminal proceeding, which were originally collected for different purpose is possible if processing of such personal data is necessary and reasonable for the purposes of criminal proceedings.

(3) The competent authority may process personal data for different purposes other than for performance of tasks for the purposes of criminal proceeding if it is compatible with the purpose for which personal data were collected and the processing for this different purpose is necessary and reasonable. Processing of personal data which has a different purpose, is regulated by a special regulation;[2)] if the personal data are processed for the purposes of activities under the jurisdiction of European union law; if the data are processed for the different purpose this Act will be governed except this Chapter of Act.

(4) If the competent authority performs the other activities than those which are related to the performance of tasks for the purposes of criminal proceeding, the processing of personal data for such purposes is governed by a special regulation[2)], if the processing of the personal data is performed within activities under the jurisdiction of European Union law; if personal data processing is not performed within the activities under the jurisdiction of European Union law, this Act will be regulated except this Chapter of Act.

Section 56
Processing of special categories of personal data

(1) Special categories of personal data may be processed by a competent authority only if:

a) data subject has manifestly given his or her personal data,

b) processing is necessary pursuant to a special regulation or an international treaty binding upon the Slovak Republic, or

c) processing is necessary to protect the life, health or property of the data subject or other natural person.

(2) The competent authority shall adopt the appropriate safeguard to protect the rights of the data subject.

Section 57

The categories of data subjects The competent authority, if possible, shall make a distinction between personal data of different categories of data subjects, in particular:

a) persons with regard to whom there are serious ground for believing that they have committed or are about to commit a criminal offence,

b) persons convicted of a criminal offence,

c) victims of a criminal offence or persons with regard to whom certain facts give rise to reason for believing that he or she could be the victim of a criminal offence,

d) other third parties to a criminal offence, particularly persons who might be called on to testify in connection with criminal proceedings, persons who can provide information on criminal offences or contact persons or associates of one of the persons refer to in points a) and b).

Section 58
The source and veracity of personal data

(1) The competent authority shall identify, if possible, personal data based on facts and personal data based on personal assessments.

(2) The competent authority prior to transmitting or transferring personal data, shall verify the accuracy, completeness and reliability of personal data, and as far as possible the competent authority shall provide measures to ensure that personal data which are inaccurate, incomplete or no longer up to date are not made available or transmitted.

(3) As far as possible, the competent authority in transmission and transformation of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness, up to date and reliability of personal data. The competent authority may not transmit and transfer incorrect personal data; the competent authority shall identify unverified personal data which are transmitting or transferring and shall specify the degree of their reliability. If the competent authority unlawfully transmits personal data or unlawfully transfers personal data or transmits incorrect personal data or transfers incorrect personal data, shall notify the recipient without delay and shall request rectify, comply or erase or restrict the processing of the personal data from recipients without delay.

TITLE TWO

RIGHTS OF THE DATA SUBJECT

Section 59

The procedure of competent authorities relating to personal data processing for performance of tasks for the purposes of criminal proceeding which is regulated by section 29 equally.

Section 60
Information to be made available or given to the data subject

(1) The competent authority shall provide on its website, particularly:

a) the identity and the contact data of competent authority,

b) the contact details of the data protection officer,

c) information about the purpose of the processing for which the personal data are intended,

d) the contact details of the Office,

e) information about the right to lodge a complaint to initiate proceedings pursuant to section 100,

f) information about the right to request from the competent authority access to and rectification, erasure or restriction of the processing of the personal data concerning the data subject.

(2) The competent authority shall give to the data subject on the based on his or her request, in specific cases, the information about:

a) the legal basis for the processing of personal data,

b) the time period for which the personal data will be stored or, where that is not possible, the criteria used to determine that period,

c) the categories of recipient of the personal data, including in third country or international organisation,

d) further information, in particular where the personal data are collected without the knowledge of the data subject.

Section 61
Right of access to the personal data

The data subject has the right to obtain from the competent authority confirmation as to whether personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:

a) the purpose of the processing of personal data and legal basis for the processing,

b) the category of personal data concerned,

c) the recipient or categories of recipient to whom the personal data have been disclosed, in particular recipient in third country or international organisation,

d) the time period for which the personal data will be stored or, if not possible, the criteria used to determine that period,

e) the right to request from the competent authority to rectification or erasure or restriction of or right to object of processing of personal data concerning the data subject,

f) the contact details of the Office,

g) the right to lodge a complaint to initiate proceedings pursuant to section 100,

h) the origin of the personal data, if available.

Section 62
Right to rectification or erasure of personal data and restriction of the rights

(1) The data subject has the right to obtain from the competent authority without undue delay the rectification of inaccurate personal data relating to him or her. Taking into account the purpose of personal data processing, the data subject has the right to have incomplete personal data completed.

(2) The data subject has the right to obtain from the competent authority to erase personal data concerning to him or her without undue delay and the competent authority must be erased it where

a) processing of the personal data is contrary to the principles of personal data processing pursuant to sections 52 to 55,

b) processing of the personal data is contrary to section 56, or

c) the erasure of the personal data is necessary for the purpose of complying the obligations with this Act, or a special regulation or international treaty binding upon the Slovak Republic.

(3) Instead of erasure, the competent authority shall restrict the processing of the personal data where:

a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained, or

b) the personal data must be maintained for the purposes of evidence.

(4) Where personal data processing is restricted pursuant to point a) of paragraph 3, the competent authority shall inform the data subject before lifting the restriction of processing of the personal data.

(5) The competent authority shall inform the data subject in writing of any refusal of right to restriction pursuant to paragraph 1, right to erasure pursuant to paragraph 2, or restriction of processing the personal data pursuant to paragraph 3, and the reason for the refusal.

Section 63
Restriction to provide of information and restriction of rights of data subject

(1) The competent authority may delay, restricted or omitted from providing information pursuant to section 60 paragraph 2, wholly or partly restricted the right to access pursuant to section 61, or wholly or partly restricted the mandatory provision of information pursuant to section 62 paragraph 5, where

a) official procedures, court proceedings or investigations could be influenced or obstructed,

b) performance of tasks for the purposes of criminal proceeding could be prosecuted,

c) it is necessary for safeguarding protection of the public order or state security, or

d) it is necessary for protecting the rights of third parties.

(2) A special regulation can set the categories of processing of the personal data to which the paragraph 1 applies.

(3) The competent authority should inform in writing the data subject if refusal or restriction of the right to access refer to section 61 and shall justify reason of this refusal or restriction; this provision shall not apply if the provision of such information could prosecute of the purpose pursuant to paragraph 1.

(4) The competent authority shall document factual or legal reasons on which restriction of the right to access pursuant to section 61 and provide them upon request to the Office.

(5) If the competent authority restricts to provide the information or restricts the right of the data subject pursuant to paragraph 1, shall inform the data subject in writing about the possibility to lodge a complaint to initiate proceedings pursuant to section 100, including the possibility to exercise the right for the Office to verify the lawfulness of the procedures taken by the competent authority pursuant to paragraphs 1 and 3 and about the possibility to exercise the rights of the data subject to other legal protection.[19)]

Section 64
Notification about rectification, erasure or restriction of personal data processing

The competent authority shall communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate. If the competent authority incorrectly rectifies, erases or restricts of processing personal data pursuant to section 62 paragraph 1 to paragraph 3, it shall notify the recipient and that the recipient shall rectify, erase or restrict the processing of the personal data.

Section 65

Provisions in sections 61 to 64 do not apply if the personal data are contained in investigation file or file under criminal proceedings; the rights listed under those provisions are exercised pursuant to a special regulation.[21)]

Section 66
Automated individual decision-making

(1) The competent authority decision which produce an adverse legal effect concerning the data subject cannot be based solely on automated processing of the personal data including profiling, unless authorised by the special regulation or international treaty which the binding upon the Slovak Republic provide otherwise. The special regulation or international treaty which the binding upon the Slovak Republic shall provide appropriate safeguards for protection of the rights of the data subject, particularly the right to obtain verification of the decision from the competent authority by non-automated means.

(2) Decision referred to in paragraph 1 shall not be based on special categories of personal data, unless suitable measures to safeguard the data subject´s rights and legitimate interests are in place.

(3) Profiling that result in discrimination against natural persons on the basis of special categories of personal data shall be prohibited.

TITLE THREE

RIGHTS AND OBLIGATIONS OF THE COMPETENT AUTHORITY AND THE PROCESSOR

Section 67

For procedure which was applied by the competent authorities when processing the personal data for performance of tasks for the purposes of criminal proceeding is regulated by section 31, section 32, section 33 paragraphs 1 and 3, section 34, section 36, section 37, sections 39 to 41, section 42 paragraphs 1 to 5 and paragraph 7 and sections 44 to 46 equally.

Section 68

(1) The competent authority shall verify once in three years if the processed personal data continue to be needed for the purposes of criminal proceedings, unless special regulation regulated otherwise.

(2) The competent authority shall maintain a records of processing activities under its responsibility. That records of processing activities shall contain except information pursuant to section 37, the following information:

a) the use of profiling, if the competent authority intends to use profiling,

b) information about the legal basis for processing activities, including the transfer for which the personal data are intended.

Section 69
Log keeping

(1) The competent authority keeps the logs for following processing operations of personal data in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of consultation or disclosure and the identification of the person who consulted or disclosed personal data, and the identity of the recipient of such personal data.

(2) The competent authority shall be used and kept the logs solely for the purposes of verification of the lawfulness of processing the personal data, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

(3) The competent authority and the processor of the competent authority shall make the logs available to the Office, if the logs are available.

Section 70
Prior consultation

(1) The competent authority shall consult the Office prior to processing personal data which will form part of a new filing system, where a data protection impact assessment as provided for in section 42 indicates that the processing would result in a high risk to the rights of the natural persons in the absence of measures taken by the competent authority to mitigate this risk or where the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to breach of the data subject’s rights.

(2) The competent authority shall provide together with a request for prior consultation, the personal data protection impact assessment pursuant to section 42, which was carried out, and on the request, with any other information to allow the Office to make an assessment of the compliance of the personal data processing with this Act and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

(3) Where the Office is of the opinion that the intended processing of personal data referred to in paragraph 1 would unlawful, in particular where the competent authority has insufficiently identified or mitigated the risks, the Office shall provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the competent authority and where applicable, to the processor. The Office may extend in accordance of previous sentence by a month, taking into account the complexity of the intended processing of personal data; the Office shall inform the controller and, where applicable, the processor of any such extension period within one month one month of receipt of the request for consultation, together with reason for the delay. The consultation period by the Office does not expire until the Office collects the information which were requested by Office under the previous consultation.

(4) Further processing operations for the competent authority which are subject to the obligation to prior consultation pursuant to paragraph 1 shall be provide a generally binding regulation issued by the Office.

Section 71
Security of processing of personal data

In respect of automated processing, the competent authority or the processor of the competent authority shall implement the following measures based on the evaluation of the risk:

a) equipment access control, in order to deny unauthorised person access to processing equipment used for processing of the personal data,

b) personal data media control, in order to prevent unauthorised reading, copying, modifications or removal of personal data media,

c) personal data storage control, in order to prevent unauthorised input of personal data to the filing system and unauthorised inspection, modification or deletion of the stored personal data in the filing system,

d) filing system user control, in order to prevent use of automated processing systems by unauthorised persons using data communication equipment,

e) personal data access control, in order to ensure that persons authorised to use automated processing system have access only to the personal data cover by their access authorisation,

f) communication control, in order to ensure it is possible to verify and establish the bodies to which personal data have been or may be transmitted, or to verify or establish the bodies to which the personal data made available using personal data communication equipment,

g) input filing system control, in order to ensure that it is possible to verify and establish which personal data have been input into automated processing system and when and by whom the personal data were input into the filing system,

h) personal data transport control, in order to prevent unauthorised reading, copying, modification or deletion of the personal data during transfer of personal data or during transportation of personal data media,

i) recovery of personal data, to ensure that installed systems will, in the case of interruption, be restored,

j) reliability of the filing system, in order to ensure that the function of the system perform and the appearance of faults in the functions is reported,

k) integrity of the filing system, in order to ensure that stored personal data cannot be corrupted by means of the system.

Section 72
Notification of a personal data breach

(1) The competent authority shall notify, without undue delay, referred to in section 40 paragraph 4, to the authority of a member state which perform tasks for the purposes of criminal proceedings, where the breach of personal data protection involves the personal data which were made by or transferred to the authority of a member state perform tasks relevant for the purposes of criminal proceedings.

(2) The competent authority may delay, restrict or omit the notification of a personal data breach to the data subject where

a) there is possibility of influencing or obstructing of official or court procedure or investigation,

b) there is possibility that performance of tasks for the purposes of criminal proceeding could be prejudiced,

c) it is necessary for ensuring the protection of the public order or state security, or

d) it is necessary for protecting the rights of other persons.

TITLE FOUR

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRY OR INTERNATIONAL ORGANISATION

Section 73

(1) Section 48 paragraph 1 and section 50 apply equally for procedures of competent authorities when processing personal data for performance of tasks for the purposes of criminal proceeding.

(2) Transfer of personal data between competent authorities and authorities of member states competent to perform tasks for the purposes of criminal proceedings is guaranteed where such transfer is required pursuant to a special regulation or international treaty by which binding upon the Slovak Republic.

Section 74
General principles for transfer of personal data

(1) The competent authority may transfer personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfer to another third country or international organisation takes place, only where:

a) the transfer is necessary for performance of tasks for the purposes of criminal proceedings,

b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent to perform tasks for the purposes of criminal proceedings, unless otherwise provided for by section 77 paragraph 1,

c) the member state has given its prior authorisation to transfer in accordance with its national law, where personal data are transmitted or made available from another member state, prior than the transfer has been made,

d) the Commission has adopted an adequacy decision pursuant to section 48 paragraph 1, or adequate guarantees have been provided or exist pursuant to section 75, or derogation for specific situations apply pursuant to section 76,

e) in the case of an onward transfer to another third country or international organisation, the competent authority that carries out the original transfer or another competent authority of the Slovak Republic authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(2) In accordance with point c) of paragraph 1 the personal data may be transferred without the prior authorisation of a member state only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to the public security of a member state or a third country, or to the essential interests of a member state and the prior authorisation cannot be obtained on good time; the authority responsible for giving prior authorisation shall be informed about prior authorisation without delay.

(3) If the competent authority transfers personal data, the processing of which requires special conditions of processing pursuant to a special regulation, shall inform the recipient about such requirements. When transferring personal data to the recipient in another member state or an agency, EU office or bodies, the competent authority shall not apply different conditions than those applicable for transfers of personal data within the Slovak Republic.

Section 75
Appropriate safeguards

(1) In the absence of a decision of the Commission on adequacy pursuant to section 48 paragraph 1, the competent authority may provide transfer of the personal data to a third country or an international organisation only where

a) appropriate safeguards with regard to the special regulation or international treaty binding upon the Slovak Republic are provided, or

b) the competent authority has assessed the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist to the protection of personal data.

(2) The competent authority shall inform the Office about categories of transfers under point b) of paragraph 1.

(3) When the competent authority take place a transfer is based on point b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the Office on request. The documentation shall specify the date and time of the transfer, information about the receiving competent authority, the justification for the transfer of personal data and the personal data transferred.

(4) Commission decision on repeal, replace or suspend its decision on adequacy referred to in section 48 paragraph 1 to be without prejudice to transfer of personal data pursuant to paragraph 1 and section 76.

Section 76
Derogation for specific situations

(1) In the absence of a Commission adequacy decision pursuant to section 48 paragraph 1 or appropriate safeguards pursuant to section 75, the competent authority may transfer of personal data to a third country or an international organisation takes place where

a) in order to protect the life, health or property of the data subject or other natural person,

b) to safeguard legitimate interests of the data subject, where it provides by a specific regulation or international treaty binding upon the Slovak Republic,

c) for to prevention of an immediate and serious threat to public security of a member state or a third country,

d) in individual cases for fulfilling tasks for the purposes of criminal proceedings, or

e) in the individual cases for the exercise of the legal claim relating to fulfilling tasks for the purposes of criminal proceedings.

(2) Personal data transfer pursuant to paragraph 1 shall not be transferred if the transferring competent authority determines that the data subject's rights concerned override the public interest in the transfer set out in the points d) and e) of paragraphs 1.

(3) Where a transfer of personal data is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the Office on request. The documentation shall specify the date and the time of the transfer, information about the receiving competent authority, the justification for the personal data transfer and the personal data transferred.

Section 77
Transfer of personal data to third-country recipients

(1) In specific cases, the competent authority may provide to transfer the personal data to recipient with its registered office, place of business, organisational unit, operating unit or permanent residence in third country if except other conditions set up by this Act for transfer of personal data

a) the transfer is necessary for the performance of a tasks for the purposes of criminal proceedings of the transferring competent authority,

b) the transferring competent authority that no rights of the data subject concerned override the public interest necessitating the transfer in the case at hand,

c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes of criminal proceedings in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time,

d) the authority that is competent to fulfil tasks for the purposes of the criminal proceedings in the third country is informed without undue delay, unless this is inefficient or inappropriate, and

e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the recipient shall process the personal data are only being processed, where such processing is necessary.

(2) The transfer to recipient from a third country referred to in paragraph 1 without prejudice an international agreement which is biding upon the Slovak Republic in the field of judicial cooperation in criminal matters and police cooperation.

(3) The transferring competent authority shall inform the Office about transfer under paragraph 1.

(4) Where the transferring competent authority transfers the personal data based on paragraph 1, such a transfer shall be documented.

CHAPTER FOUR

SPECIFIC SITUATIONS OF LAWFULL PROCESSING OF PERSONAL DATA

Section 78

(1) The controller may process personal data without consent of data subject where this processing is necessary for the academic purpose, artistic purpose or literary purpose; this shall not apply where the controller by processing for that purpose, violates the right of data subject to the protection of his or her person or the right to privacy, or where such processing without consent of data subject is excluded by a special regulation or an international treaty binding upon the Slovak Republic.

(2) The controller may process personal data without consent of data subject where this processing is necessary to inform the public by mass media means and where the personal data are processed by a controller based on its field of activity; this shall not apply where controller, by processing for that purpose, violates the right of data subject to the protection of his or her person or the right to privacy, or where such processing without consent of data subject is excluded by a special regulation or an international treaty binding upon the Slovak Republic.

(3) The controller that is an employer of the data subject is allowed to make available or make public his or her personal data to the extent of degree, name, surname, job position, public service job, function, identification number of an employee or employee number, department, place of work, phone number, fax number, company e-mail address of that employee and identifying information of the employer where necessary in connection with fulfilment of the tasks within that data subject's employment, service job, or function. The making available or making public personal data shall not violate the respectability, dignity, and security of the data subject.

(4) During processing, a generally applicable identifier referred to in special regulation[22)] may only be used to identify a natural person where the use of such identifier is necessary to achieve the purpose of this processing. The consent to the processing of generally applicable identifier shall be express and shall not be excluded under special regulation, where the legal basis for the processing is based on the consent of data subject. Making public of general applicable identifier shall be prohibited; however, its shall not apply where such general identifier is disclosed by the data subject himself or herself.

(5) The controller may also process genetic data, biometric data or data concerning to health on a legal basis under a special regulation or an international treaty binding upon the Slovak Republic.

(6) The personal data of data subject can only be collected from another natural person and processed in the filing system only with prior written consent of data subject; this shall not apply where by making available personal data on the data subject in the information system, another natural person protects his or her rights or interests protected by law, notifies the facts justifying the person's legal liability or where the personal data are processed based on a special Act referred to in the point c) and e) of section 13 paragraph 1. Those who process such personal data shall be able to demonstrate to the Office at its request that such personal data were collected in compliance with this Act.

(7) If the data subject dies, the consent requested under this Act or under special regulation[2)] may be given by a close person to him or her.[23)] The consent shall not be valid if at least one close person gave a written disapproval.

(8) Where personal data are processed for archiving purpose, scientific purpose or historical research purpose or statistical purpose, controller and processor shall implement reasonable safeguards to protect the rights of data subject. Those safeguards shall involve that appropriate and effective technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation and pseudonymisation.

(9) Where the personal data are processed for scientific purpose or historical research purpose or statistical purpose, the data subject's rights referred to in sections 21, 22, 24 and 27 or in a special regulation[24)] may be restricted by special regulation or an international treaty binding upon the Slovak Republic, provided that appropriate conditions and safeguards referred to in paragraph 6 have been implemented, where such data subject's rights are likely to render impossible or seriously impair the achievement of such purposes, and such restriction of rights of data subject is necessary for achievement of such purposes.

(10) Where personal data are processed for archiving purpose, the data subject's rights referred to in section 21, section 22, sections 24 to 27 or in a special regulation[25)] may be restricted by special regulation, where appropriate conditions and safeguards referred to in paragraph 6 have been implemented, if such data subject's rights are likely to render impossible or seriously impair the achievement of such purposes, and such restriction of rights of data subject is necessary for achievement of such purposes.

(11) When taking security measures and assessing the impact on personal data protection, the controller and processor shall apply international norms and security standards, in adequacy manner.

Section 79
Secrecy

(1) The controller and processor shall keep an obligation of secrecy of personal data processed by them. The obligation of secrecy shall remain valid after the end of personal data processing.

(2) The controller and processor shall impose the obligation of personal data secrecy on natural persons who come in contact with personal data in the place of controller or processor operation. The obligation of secrecy referred to in the first sentence shall remain after the termination of the employment contract, public servant contract, civil service contract, or a similar labour relationship of that natural person.

(3) The obligation of secrecy referred to in paragraphs 1 and 2 shall not apply, where necessary for the performance of the tasks of a court or law enforcement authorities pursuant to special Act; this shall not apply to the provisions concerning secrecy referred to in special regulations.[26)]

(4) The provisions concerning the obligation of secrecy referred to in paragraphs 1 and 2, section 45 paragraph 5 shall not apply in relation to the Office while the Office performs its tasks under this Act or special regulation.[2)]

CHAPTER FIVE

THE OFFICE

TITLE I

STATUS, SCOPE AND ORGANISATIONAL STRUCTURE OF THE OFFICE

Section 80
Status of the Office

(1) The Office is a state administration body with national jurisdiction over the territory of the Slovak Republic, that participates in the protection of fundamental rights of natural persons in relation to processing of personal data and executes data protection supervision, including supervision of personal data protection by competent authorities for performance of the task for the purposes of criminal proceedings, unless section 81 paragraphs 7 and 8 provides otherwise.

(2) The headquarter of the Office is Bratislava.

(3) The Office for the performance of task for supervision authority of the data protection may establish and close branches outside the headquarter of Office and may identify their geographical jurisdiction.

(4) The Office, when exercising its jurisdiction, acts independently and is governed by Constitution of the Slovak Republic, constitutional act, acts, other generally binding legal regulations and international treaties binding upon the Slovak Republic.

(5) The Office is a budgetary organisation.[27)] The Office submits its proposal budget as a part of the General Treasury Administration chapter. Only the National Council of Slovak republic may decrease the approved budget of the Office during a calendar year.

(6) The organisational details shall be regulated by the Organisational Structure of the Office issued by president of the Office.

Section 81
Tasks of the Office

(1) The Office is a supervisory authority pursuant to this Act or special regulation[28)], and perform tasks and exercise powers that were entrusted to the it pursuant to a specific regulation.[29)]

(2) The Office

a) monitors the implementation of this Act,

b) comments on drafts of Acts and drafts of generally binding regulations governing the processing of personal data,

c) provides consultation in the area of the protection of personal data,

d) provides methodological guidelines on personal data processing to controllers and processors,

e) promote public awareness, in particular on risks and rights in relation to processing of personal data,

f) promote the awareness of controllers and processors on their obligations under this Act,

g) upon request, provides information to any data subject concerning the exercise of their rights under this Act and cooperates with supervisory authorities of other Member States for this purpose,[30)]

h) in the exercise of supervision over the protection of personal data, it verifies the lawfulness of processing of personal data by the competent authorities in exercising rights by a data subject pursuant to section 63 paragraph 5 and informs the data subject about the results of the verification within 30 days of the date of submission of the request for verification, or of the reasons why the verification was not carried out, and of the possibility to exercise the data subject's right to lodge a complaint to initiate proceedings pursuant to section 100 and for other type of legal protection pursuant to specific regulation,[19)]

i) monitors development, in particular the development of information and communication technologies and commercial practices if they have any impact on the protection of personal data,

j) cooperates with the European Data Protection Board in the area of personal data protection,[31)]

k) submits to the National Council of Slovak Republic a report on state of protection of personal data at least once a year; the report on the state of personal data protection is published by the Office on its website and provides it to the European Data Protection Board and to the Commission,

l) cooperates with supervisory authorities of other member states, including the exchange of information, and provides them with mutual assistance in order to ensure a common approach to the protection of personal data under this Act and the special regulation.[32)]

(3) For performance of the task, the Office is authorised

a) to order the controller and processor, or representative of controller or processor if so authorised, to provide information essential for performance of its tasks,

b) to obtain from the controller and the processor access to personal data and information that are necessary for performance of its tasks; the provision of secrecy pursuant to special regulations remain unaffected,[26)]

c) to enter the premises of a controller and processor, as well as any equipment and means for processing personal data, to the extent necessary for the performance of his tasks, unless permission is required under a special regulation,[33)]

d) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions adopted pursuant to this Act or special regulations,[2)]

e) to impose measures for liability, a fine pursuant to section 104 or administrative fine pursuant to section 105 if the controller, processor, monitoring body or certification body infringes the provisions of this Act or special regulations,[2)]

f) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Act or special regulations,[2)]

g) to order the controller or processor to bring processing operations into compliance in a specified manner and within a specified period with the provisions of this Act or special regulations,[2)]

h) to order the controller to communicate a personal data breach to the data subject,

i) to impose a temporary restriction or definitive restriction of personal data processing,

j) to ask the controller or processor to give an explanation in case of suspicion of an infringement of obligation under this Act, a special regulation or international treaty binding upon by the Slovak Republic,

k) to recommend the controller or processor adopt measures for ensuring protection of personal data in the filing systems,

l) to order the suspension of data flows to a recipient in a third country or an international organisation.

(4) The Office except the performance of the tasks under paragraphs 1 and 2 carries out the following:

a) fulfils the notification obligation for the Commission in the field of personal data protection,

b) adopts the measures to execute decisions of the Commission, which was issued in the field of personal data protection,

c) cooperates with the supervisory authorities of other member states and with similar supervisory authorities outside the territory of member states in the supervision of personal data protection.

(5) The subject of supervision over the protection of personal data is not disputes arising from contractual relations or pre-contractual relations between the controller or the processor and the data subject or other persons whose courts and other bodies are competent to hear and decide under special regulations.(6) The Office may charge a reasonable fee based on administrative costs or refuse to act on the request if the manifestly unfounded or excessive character of the complaint, in particular because of their repetitive character. The Office shall bear the burden demonstrating the manifestly unfounded or excessive character of the complaint.

(7) Where personal data are processed by the courts when acting in their judicial capacity, personal data protection supervision is exercised by the Ministry of Justice of the Slovak Republic pursuant to sections 90 to 98.

(8) Where personal data are processed by the National Security Authority pursuant to a special regulation,[5)] supervision pursuant to sections 90 to 98 is exercised by the National Council of Slovak Republic pursuant to a special regulation.[34)]

Section 82
President of the Office

(1) The Office is headed by the president, who is elected and recalled by the National Council of the Slovak Republic upon proposal of the Government of the Slovak Republic.

(2) The term of office of the president is five year and the president may be elected for

maximally in two consecutive terms. The president remains in office even after the term of office has expired until the National Council of Slovak Republic elects a new president.

(3) Any citizen of the Slovak Republic, who is eligible for a deputy of the National Council of the Slovak Republic, with university education of the second degree, a minimum of two years' experience in personal data protection and has no criminal record, may be elected by the National Council of Slovak Republic as president of the Office.

(4) For the purpose of this Act, person with integrity is who has not been lawfully sentenced for an intentional criminal offence or for criminal offence or for a criminal offense where the imprisonment was not conditionally suspended, if it is not judged by the court or by act, as if it were not convicted or sentenced. The integrity of the person is demonstrated by the extract from criminal record not older than three months.

(5) The president of the Office shall be an independent in the performance of his duties and shall not be under external influence, whether direct or indirect, and shall neither seek nor take instructions from anyone in the performance of his duties and powers under this Act.

(6) The president of the Office shall abstain from any acting incompatible with his or her obligations pursuant to this Act and a special regulation.[35)]

(7) The president of the Office is a civil servant pursuant to a special regulation.[7)] The president is entitled to a monthly salary, which is equal to four times of the average nominal monthly salary of the employee in the national economy of Slovak Republic for the previous calendar year rounded up to the nearest euro. Salary and other matters related to the position of the president of the Office are decided by the Government of Slovak republic.

(8) The office of president of the Office shall cease to exist upon expiry of his term of office or upon the election of a new president after the expiry of the term of office of the president of the Office under paragraph 2.

(9) Before the expiry of the term of office, the performance of the function ceases

a) by resigning from the function,

b) by losing eligibility for election to the National Council of Slovak Republic,

c) upon the entry into force of the judgment which has been convicted of an intentional criminal offense or for which he has been convicted of an offense and has not been conditionally suspended,

d) by performing of activity incompatible with his or her duties as specified under paragraph 6, or

e) by death or by a final decision of the court to declare the president of the Office dead.

(10) The president of the Office may be recalled from the function if

a) his or her health condition does not allow him or her to perform his or her obligations arising from the function on a long-term basis, but at least for a period of one year,

b) he or she has infringed the independency pursuant to paragraph 5, or

c) he or she has infringed the secrecy obligation in relation to the facts which he or she had known about in connection with performance of its function pursuant to Section 84.

Section 83
Vice-president of the Office

(1) The president of the Office shall be represented by the vice-president of the Office, who shall be elected and recalled by the Government of Slovak Republic upon proposal by the president of the Office. The vice-president is a civil servant pursuant to a special regulation.[7)]

(2) The function term of office of the vice-president is five years and he or she may be elected for at most two consecutive terms. The vice-president shall remain in the function also after the his or her term of office expired until the Government of the Slovak Republic elects another vice-president.

(3) The provisions of Section 82 paragraphs 3 to 6 and paragraphs 8 to 10 shall apply for the performance of the vice-president´s functions.

Section 84
Obligation of secrecy

(1) The president, vice-president and employees of the Office shall maintain professional secrecy about facts they have known during performing their working tasks pursuant to this Act or special regulations,[2)] also after termination of their position, civil service or similar working relationships.

(2) The obligation of secrecy in refer to paragraph 1 is not applied if it is necessary for the performance of court tasks or law enforcement authorities pursuant under special regulations[36)] provisions of secrecy pursuant to specific regulations[37)] remain unaffected.

(3) The president of the Office may exempt the obligation of secrecy refer to paragraph 1 for the vice-president and employees of the Office. The National Council of Slovak Republic may exempt the obligation of secrecy refer to paragraph 1 for the president in specific case.

TITLE II

CODE OF CONDUCT, CERTIFICATE AND ACCREDITATION

Section 85
Code of Conduct

(1) An association which represents the category of the controllers or processors or any other bodies which represents the category of the controllers or processors may adopt a code of conduct, particularly for the purpose of specifying the application of this Act or special regulation[2]) in relation to the subject-matter of the code of conduct as referred to in a special regulation.[38])

(2) The approval of a code of conduct by Office shall not affect the responsibility of the controller or processor for compliance with this Act or a special regulation.[2])

(3) The application for approval of the draft code of conduct, the draft amendment to approved code of conduct or the draft extension of the approved code of conduct shall be submitted to the Office by the association or other body referred to in paragraph 1 (hereinafter "applicant").

(4) The application for approval of a code of conduct shall contain

a) applicant's identifying information;

b) name and surname of a statutory body or of a person authorised to act on applicant's behalf;

c) indication whether it is a draft code of conduct, a draft amendment to approved code of conduct or draft extension of approved code of conduct;

d) the association's procedure, by which a member of the association agrees to comply with the approved code of conduct;

e) the controller´s or processor´s commitment to submit to the monitoring of compliance with the approved code of conduct pursuant to the rules and procedures to monitor compliance with the code of conduct;

f) description of the rights and obligations of the controller or processor during the monitoring of compliance with an approved code of conduct;

g) specification of the subject-matter to which a draft code of conduct, draft amendment to approved code of conduct or draft extension of approved code of conduct shall relate;

h) the purpose of processing for which the personal data are intended, and the legal basis for personal data processing;

i) the categories of personal data;

j) the categories of data subjects;

k) identification of the recipient or a category of the recipient of the personal data, if any;

l) description of processing activities, information concerning existence of automated decision-making and information about the existence of profiling;

m) description of applicant's procedures used in exercise of rights of a data subject;

n) information whether the draft code of conduct relates to processing activities in several Member States;

o) identification of the third country or an international organisation when transferring personal data and information about appropriate safeguards adopted for such transfer;

p) measures and procedures adopted to monitor compliance with the code of conduct.

(5) Besides the application for approval of a code of conduct referred to in paragraph 4, the applicant shall also submit

a) a draft code of conduct, a draft amendment to approved code of conduct or draft extension of approved code of conduct; when it relates to the processing activities in several Member States, English language version is also required;

b) confirmation of an administrative fee payment;

c) other information and documents necessary for assessment of compliance the draft code of conduct with this Act or special regulation.[2])

(6) Where the application for approval of a code of conduct fails to meet the requirements referred to in paragraphs 4 and 5 or where doubts occur during the code approval proceeding

with regard to establishment of compliance with this Act or special regulation[2]), the Office shall ask the applicant to provide additional documents in a period that shall not be shorter than 15 days; the code approval proceeding period does not run during this period.

(7) The party to the code approval proceeding is the applicant who filed an application referred to in paragraph 4.

(8) Where the Office, during the code approval proceeding, identifies a non-compliance with this Act or special regulation[2]), the Office shall ask the applicant to remove the identified non-compliance within a specific time period that shall not be shorter than 30 days; the period in the code approval proceeding does not run for the period granted for removal of the identified non-compliance. The Office may extend this period by a maximum of 60 days on the basis of the reasoned applicant´s request.

(9) The code approval proceeding shall be stopped by the Office where the applicant

a) does not remove deficiencies in the application within the period set in paragraph 6;

a) does not remove deficiencies identified by the Office within the period set in paragraph 8.

(10) The Office shall decide about the approval of a code of conduct, an amendment to approved code of conduct or extension of approved code of conduct up to 90 days from the day of initiation of the proceeding.

(11) Where a draft code of conduct, a draft amendment to approved code of conduct or an extension of approved code of conduct needs to be submitted to the European Data Protection Board as referred to in special regulation,[39]) the time period referred to in paragraph 10 does not run from the date of submitting a draft code of conduct, or a draft amendment to approved code of conduct, or draft extension of approved code of conduct, to the European Data Protection Board to the day when the opinion of European Data protection Board is delivered to the Office as referred to in special regulation[40]).

(12) The Office shall issue, after reviewing the application for approval of a code of conduct as referred to in paragraphs 4 and 5 and the related documentation, a decision on the approval of a code of conduct, decision on amendment to approved code of conduct or extension of approved code of conduct, if the draft code of conduct, draft amendment to approved code of conduct or draft extension of approved code of conduct is in compliance with, and provides appropriate safeguards for the protection of personal data as referred to in this Act or special regulation.[2])

(13) There is no appeal against decision on the approval of a code of conduct, decision on amendment to approved code of conduct or extension of approved code of conduct.

(14) An appeal may be submitted against decision on disapproval of a code of conduct, decision on the disapproval of an amendment to approved code of conduct, or decision on the disapproval of extension of approved code of conduct; such appeal shall be decided by the president of the Office.

(15) The Office shall publish a list of approved codes of conduct on its web site.

(16) The association which represents the category of controllers or processors or any other body which represents the category of controllers or processors whose code of conduct, draft amendment to approved code of conduct or draft extension of approved code of conduct was approved by the Office, shall notify the Office in writing of any changes as referred to in points a) and d) of paragraph 4 no later than in 15 days from the date of detection.

Section 86
Certificate

(1) The issuance, renewal or withdrawal of certificate is carried out by an accredited entity as referred to in section 88 in accordance with this Act (hereinafter as "certification body") or by the Office.

(2) The controller or processor, for the purposes of the compliance of personal data processing and existence of appropriate safeguards to protect personal data pursuant to this Act or special regulation[2]), may apply the Office or a certification body to issue or renew the certificate. The certificate shall be issued or renewed for a maximum period of three years.

(3) The Office or the certification body shall assess the compliance of personal data processing and the existence of appropriate safeguards to protect personal data of a controller or processor as referred to in paragraph 2 based on certification criteria pursuant to this Act. The issue of certificate shall not affect the responsibility of the controller or processor for compliance with this Act and special regulation[2]), or to the powers of the Office under this Act.

(4) The certificate is a public document.

(5) The Office shall publish issued certificates on its website.

(6) An application for issuing certificate or an application for renewing certificate by the Office shall contain

a) applicant's identifying information;

b) name and surname of a statutory body of applicant or of a person authorised to act on applicant's behalf;

c) contact details of data protection officer, if determined;

d) the subject-matter of certificate for which the certificate is to be granted;

e) the purpose of personal data processing;

f) the legal basis for the processing of personal data;

g) the categories of data subjects;

h) the categories of personal data;

i) identification of recipient or category of recipient of personal data, if any;

j) description of processing activities, including information concerning existence of automated decision-making including profiling;

k) description of an applicant's actions in exercising the rights of data subject;

l) identification of a third country or an international organisation when transferring personal data.

(7) The applicant shall attach to the application referred to in paragraph 6

a) technical and security documentation necessary for issuing a certificate;

b) the data protection audit result not older than six months;

c) documents proving compliance with certification criteria;

d) description of appropriate safeguards when transferring personal data to the third country or an international organisation;

e) confirmation of an administrative fee payment;

f) further information and documents necessary to assess the compliance with this Act or special regulation[2]) and compliance with the certification process.

(8) If the application for issuing certificate or application for renewing certificate does not meet the requirements referred to in paragraphs 6 and 7 or where doubts arise with regard to the proof of the compliance with certification criteria or fulfilment of the conditions for issuing certificate during the certification issuing proceeding or certification renewing proceeding, the Office shall ask the applicant to provide additional documents within a time period that shall not be shorter than 15 days; the period in the certification issuing proceeding or certification renewing proceeding does not run during this time.

(9) If, during the certification issuing proceeding or certification renewing proceeding, the Office identifies a non-compliance with this Act or special regulation[2]), the Office shall ask the applicant to remove the non-compliance found within a specific time period that shall not be shorter than 30 days; the period in the certification issuing proceeding or certification renewing proceeding does not run during this time. The Office may extend this period by a maximum of 60 days on the basis of the reasoned applicant´s request.

(10) The certification issuing proceeding or certification renewing proceeding shall be suspended by the Office where the applicant does not remove

a) deficiencies in the application and doubts arisen as referred in paragraph 8 within the specified period,

b) deficiencies identified by the Office as referred to in paragraph 9 within the specified period.

(11) The Office shall decide about issuing or renewing the certificate up to 90 days from the day of initiation of the proceeding.

(12) The Office shall adopt a decision on issuing certificate, after reviewing the application for issuing certificate or application for renewing certificate as referred to in paragraphs 6 and 7 and the related documentation, if the applicant has met the certification criteria, requirements of certification procedure, if applicant's processing activities are in compliance with this Act or special regulation[2]) and if the security measures taken by the applicant provide appropriate safeguards for the protection of personal data under this Act or special regulation.[2])

(13) The Office, based on a decision approving the issuance or renewal of a certificate shall issue a certificate for the applicant for a period of three years which shall contain

a) Office's identifying information;

b) applicant's identifying information;

c) subject-matter of the certificate;

d) identification of certification criteria based on which the certificate has been issued;

e) certificate number;

f) certificate issue date; or, where renewal of certificate, also the earlier issue date of the certificate;

g) certificate validity period;

h) the imprint of the official stamp of the Office and the signature of the person authorised to act on behalf of the Office stating his or her name, surname, and academic degree.

(14) There is no appeal against the decision on issuing certificate or decision on renewing certificate.

(15) Appeal may be submitted against the decision on not issuing certificate or decision on not renewing certificate, and such appeal shall be decided by the president of the Office.

(16) Where controller or processor that was issued or renewed a certificate (hereinafter as "certified person") continues to meet the certification criteria and requirement of issuing certificate under this Act, the Office shall decide on the renewal of a certificate for additional three years based on an application of the certified person lodged no later than six months prior to expiry of the certificate issued or renewed on an earlier date. The provisions on the issuing the certificate shall apply mutatis mutandis in the certificate renewal proceeding.

(17) If the certified person submits an application for renewing certificate in a shorter period than six months prior to expiry of the certificate validity period, the Office shall disregard the application. This shall be without prejudice to the right of the certified person to submit an application for issuing certificate as referred to in paragraphs 6 and 7.

(18) During the validity of the certificate, the certified person shall

a) meet the requirements laid down under this Act and the requirements for issuing certificate in accordance with the decision on issuing certificate;

b) no later than up to 15 days from the day when any change happened, notify the Office in writing of any changes relating to the decision on issuing certificate;

c) allow the Office to exercise audit pursuant to this Act;

d) archive documentation related to the compliance with the exercising of certification procedure under special regulation.[41])

(19) The certification criteria, requirements of certification procedure, requirements for the content of technical and security documentation, and the conditions for audit of personal data protection including the conditions for auditor´s professional knowledge of an auditor conducting data protection supervision shall be laid down in a generally binding legal regulation, issued by the Office.

Section 87
Monitoring Body

(1) Monitoring of compliance of the personal data processing pursuant to this Act or special regulation[2]) with the code of conduct shall be carried out by a body that meets the criteria and conditions for granting accreditation pursuant to this Act or special regulation[2]) and was

granted an accreditation by the Office in compliance with this Act (hereinafter as "monitoring body").

(2) The codes of conduct approved by the Office for public authorities and public institutions are not subject to the activities carried out by the monitoring body pursuant to this Act; this shall be without prejudice to the supervision exercised by Office pursuant to this Act.

(3) The monitoring body may be a legal or natural person – entrepreneur that has technical and organisational conditions to carry out monitoring of the code of conduct and was granted an accreditation.

(4) Monitoring body is empowered

a) to monitor the compliance of personal data processing with this Act or special regulation[2]) by a controller or processor that is a member of an association committed to comply with an approved code of conduct;

b) to take appropriate measures in the event of violation of the code of conduct by the controller or processor;

c) to temporary suspend an approved code of conduct, for the controller or processor that has committed to comply with an approved code of conduct;

d) to withdraw binding nature of an approved code of conduct to the controller or processor that has committed to comply with an approved code of conduct.

(5) The monitoring body shall notify the Office in writing of the measures referred to in paragraph 4, including the reasons for the adoption of such measures, within 15 days from its adoption. This shall be without prejudice to the responsibility of controller or processor that is subject of monitoring of a code of conduct to comply with this Act or special regulation.[2])

(6) The application for granting accreditation shall contain

a) applicant's identifying information;

b) name and surname of a statutory body of applicant or a person who is authorised to act on applicant's behalf;

c) subject-matter of the code of conduct.[38])

(7) The applicant shall attach to the application referred to in paragraph 6

a) technical and security documentation necessary for monitoring of the code of conduct;

b) documents proving applicant's independence;

c) a procedure and method of handling a conflict of interest between the applicant and the entity subject to monitoring that could violate or restrict objectiveness of the monitoring of code of conduct, or that could interfere the principle of transparency for the data subject and the public; a conflict of interest means, in particular, a situation when the applicant who may affect the result or process of monitoring of code of conduct has a direct financial interest or indirect financial interest, an economic interest or other personal interest which can be considered to jeopardize its independence in relation to the monitoring of the code of conduct;

d) documents establishing qualification requirements in relation to the monitoring of the code of conduct for applicant's persons who shall carry out the monitoring activity;

e) rules and processes for the carrying out of activities, particularly the processes of monitoring the compliance with the code of conduct of controller or processor, the method used to prove compliance with the code of conduct of controller or processor, the method to prove compliance of processing activities of controller and processor in relation to the subject-matter of the code of conduct, frequency of compliance monitoring;

f) documents proving that the rules and processes of the code of conduct monitoring are transparent for the data subject and the public;

g) result of the code of conduct monitoring audit;

h) confirmation of an administrative fee payment;

i) further information and documents necessary to assess the compliance with this Act or special regulation[2]) and to assess the application for granting accreditation.

(8) Where the application for granting accreditation fails to meet the requirements referred to in paragraphs 6 and 7 or where doubts occur during accreditation granting proceeding with regard to establishment of compliance with criteria or conditions for accreditation, the Office shall ask the applicant to remove deficiencies in a period not shorter than 15 days; the period for the accreditation granting proceeding does not run during that time.

(9) If the Office identifies a non-compliance with this Act or special regulation[2]) during the proceeding referred to in paragraph 11, the Office shall ask the applicant to remove the identified non-compliance within a specific time period that shall not be shorter than 30 days; the period referred to in paragraph 11 does not run during that time. The Office may extend this period by a maximum of 60 days on the basis of the reasoned applicant´s request.

(10) The proceeding referred to in paragraph 11 shall be stopped by the Office where the applicant does not remove

a) deficiencies in the application and doubts arising under paragraph 8 within the specified time period;

b) deficiencies which were found by the Office as referred to in paragraph 9 within the specified time period.

(11) The Office shall decide on granting the accreditation up to 90 days from the day of initiation of the proceeding.

(12) After reviewing the application for granting accreditation referred to in paragraphs 6 and 7 and the related documentation by the Office, the Office shall adopt the decisions on granting accreditation, if the applicant meets requirements, has appropriate level of expertise in relation to the subject-matter of the code of conduct, and meets the criteria and conditions for granting accreditation laid down under this Act.

(13) Based on decision on granting accreditation, the Office shall issue a declaration on granting accreditation for the monitoring body which shall contain

a) Office's identifying information;

b) applicant's identifying information;

c) subject-matter of the accreditation;

d) number of the declaration on granting accreditation;

e) issue date of the declaration on granting accreditation;

f) imprint of the official stamp of the Office and signature of the person authorised to act on behalf of the Office stating his or her name, surname and position.

(14) Declaration on granting accreditation is a public document.

(15) There is no appeal against decision on granting accreditation.

(16) The appeal may be submitted against decision on not granting accreditation, and such appeal shall be decided by the president of the Office.

(17) The Office shall publish issued declarations on granting accreditation on its web site.

(18) If the monitoring body is proved to carry out monitoring of a code of conduct in contrary to this Act or special regulation[2]), good manners, declaration on granting accreditation, or does not meet requirements for granting accreditation any more, the Office shall suspend the validity of accreditation for three months and impose obligations for the monitoring body to remedy the situation. If the monitoring body fails to take measures specified above, the Office shall withdraw the accreditation based on a decision. The monitoring body to which accreditation has been withdrawn may re-apply for granting accreditation.

(19) Monitoring body shall

a) meet the requirements laid down under this Act and the accreditation requirements in accordance with decision on granting accreditation;

b) notify the Office in writing of any changes of the granting accreditation within 15 days from the date of a change;

c) inform the affected controller or processor of the eligibility to monitor compliance with the code of conduct and of the subject-matter of the monitored code of conduct, inform in a detailed and clear manner of security measures, rules and procedures of monitoring of code of conduct, and inform of possible legal consequences of monitoring of the compliance with the subject-matter of the code of conduct prior to monitoring of the approved code of conduct;

d) inform, without any undue delay, the affected controller or processor of measures taken, if a violation of the code of conduct of the affected controller or processor as referred to in paragraph 4 was found;

e) adhere to the principle of independence;

d) archive documentation relating to the monitoring of the code of conduct under special regulation.[42])

(20) The criteria for granting accreditation, requirements of accreditation procedure, requirements for the content of technical and security documentation, and the conditions for exercise of audit over the monitoring of code of conduct including the conditions auditor´s professional knowledge shall be laid down in a generally binding legal regulation to be issued by the Office.

Section 88
Certification Body

(1) The issuance, renewal or withdrawal of the certificate is carried out by a certification body

that meets criteria and requirements for granting accreditation referred to in this Act or special regulation[43]) and that accreditation was granted by the Office in accordance with this Act.

(2) Certification body may be a legal person or a natural person – entrepreneur that has an appropriate level of expertise in relation to the protection of personal data and has established technical and organisational conditions for the certification procedure and that an accreditation was granted.

(3) The certification body shall be responsible for assessing the compliance of personal data processing and of the existence of appropriate safeguards to protect personal data as referred to in this Act or special regulation[2]) of the controller or processor, based on which the certificate shall be granted, renewed or withdrawn.

(4) The application for granting accreditation shall contain

a) applicant's identifying information;

b) name and surname of a statutory body or a person authorised to act on applicant's behalf;

c) subject-matter of certification criteria.

(5) The applicant shall attach to the application referred to in paragraph 4

a) technical and security documentation necessary for the certification procedure;

b) a procedure and method of handling a conflict of interest between the applicant and the controller or processor that applied for issuance or renewal of certificate that could violate or restrict objectiveness of the issuance or renewal of certificate process, or that could infringe the principle of transparency for the data subject and the public; a conflict of interest means, in particular, a situation when the applicant that may influence the result or process of a certificate issuance or renewal process has a direct financial interest or indirect financial interest, an economic interest or other personal interest that can be considered to its independence in relation to the certificate issuance or renewal process;

c) documents laying down qualification requirements in relation to the certification procedure of persons who shall carry out the certification procedure on behalf of the applicant;

d) rules and processes of the certification procedure including the procedure for issuing a certificate, regular review, renewal and withdrawal of the certificate;

e) declaration of compliance with certification criteria for certification procedure;

f) documents proving processes and rules of handling of complaints relating to violations of a certificate issued or to the method of exercise of the powers out of the certificate by the relevant controller or processor;

g) documents proving that the complaint handling rules and processes in relation to the certificates issued are transparent in the eyes of the public;

h) result of the certification procedure audit;

i) confirmation of an administrative fee payment;

j) further information and documents necessary to assess the compliance with this Act or special regulation[2]) to assess the application for granting accreditation.

(6) Where the application for granting accreditation fails to meet the requirements referred to in paragraphs 4 and 5 or where doubts occur that criteria and requirements for granting accreditation are met in proceeding pursuant to paragraph 9, the Office shall ask the applicant to remove deficiencies in a period that shall not be shorter than 15 days; the period referred to in paragraph 9 does not run during this time.

(7) If, during the proceeding referred to in paragraph 9, the Office identifies a non-compliance with this Act or special regulation[2]), the Office shall ask the applicant to remove the non-compliance found in a specific time period that shall not be shorter than 30 days; the period in the accreditation granting proceeding does not run during this time. The Office may extend this period by a maximum of 60 days on the basis of the reasoned applicant´s request.

(8) The accreditation granting proceeding shall be stopped by the Office where the applicant fails to remove

a) within the time period specified, deficiencies of the application and doubts arisen as referred in paragraph 6;

b) within the time period specified, deficiencies found by the Office as referred to in paragraph 7.

(9) The Office shall decide on granting the accreditation within 90 days from the day of initiation of the proceeding.

(10) After reviewing the application for granting accreditation referred to in paragraphs 4 and 5 and the related documentation, the Office shall issue an accreditation granting decision and approve the certification criteria, provided that the applicant meets requirements for an appropriate level of expertise in relation to the protection of personal data, and meets the criteria and requirements for granting accreditation laid down under this Act.

(11) Based on an accreditation granting decision, the Office shall issue declaration on granting accreditation for five years for the certification body that shall contain

a) Office's identifying information;

b) applicant's identifying information;

c) subject-matter of the accreditation;

d) number of the declaration on granting accreditation;

e) declaration on granting accreditation issue date; where the accreditation is being renewed, also the earlier accreditation date;

e) validity period of the declaration on granting accreditation;

g) the imprint of the official stamp of the Office and the signature of the person authorised to act on behalf of the Office stating his or her name, surname, and academic degree.

(12) The declaration on granting accreditation is a public document.

(13) Appeal may not be submitted against decision on granting accreditation.

(14) Appeal may be submitted against decision on not granting accreditation, and such appeal shall be decided by the president of the Office.

(15) The Office shall publish a list of certification bodies and the approved certification criteria on its web site.

(16) If the certification body meets the requirements for appropriate level of expertise in relation to the protection of personal data, meets the criteria and requirements for granting accreditation under this Act, the Office shall decide to renew the accreditation for the next five-year period based on an application filed by the certification body for renewal of accreditation no later than six months before expiry of the declaration on granting accreditation. The provisions treating accreditation granting proceeding shall apply, *mutatis mutandis*, to the accreditation renewing proceeding.

(17) Applications for renewing accreditation filed by the certification body in a shorter period than six months prior to expiry of the declaration on granting accreditation shall be disregarded by the Office. This shall be without prejudice to the right of that body to file an application referred to in paragraphs 4 and 5.

(18) If the certification body is proved to carry out certification procedure and the certification granting and withdrawing contrary to this Act or special regulation,[2]) principles of morality, declaration on granting accreditation issued, or does not meet the accreditation requirements any more, the Office shall suspend the validity of accreditation for three months and impose an obligation on the certification body to remedy the situation. If the certification body fails to take measures specified, the Office shall withdraw the accreditation based on a decision. The subject to which the accreditation was withdrawn may apply for granting accreditation again.

(19) The accreditation criteria, conditions of accreditation procedure, certification criteria, requirements for the content of technical and security documentation, and the conditions for audit of the certification procedure including the conditions for auditor´s professional knowledge shall be laid down in a generally binding legal regulation to be issued by the Office.

Section 89
Obligations of Certification Body

(1) To the extent permitted under declaration on granting accreditation, the certification body may issue or renew a certificate to controller or processor for a period of three years.

(2) Prior to certificate issuance or renewal, the certification body shall inform the Office of

a) its identifying information;

b) number of the declaration issued to that body;

c) identifying information of controller or processor that has applied for issuing certificate, or of the certified person that has applied for renewing certificate;

d) subject-matter of the certificate;

e) certification criteria;

f) reasons for issuing or renewing certificate.

(3) If the notification fails to contain the particulars referred to in paragraph 2, the Office shall ask the certification body to remove the deficiencies in a time period that shall not be shorter than 15 days; the period referred to in paragraph 4 does not run during that time.

(4) The Office shall decide on permission for issuing certificate or permission for renewing certificate by certification body in 60 days from initiation of the proceeding.

(5) In a proceeding referred to in paragraph 4, the Office does not assess compliance with certification criteria, or with the conditions for issuing or renewing certificate.

(6) Permission of Office for issuing certificate or permission of Office for renewing certificate for the certification body shall not be to the prejudice to the responsibility of the relevant controller or processor for compliance with this Actor special regulation.[2])

(7) If, during the permission issuing certificate proceeding or permission renewing certificate proceeding by the certification body, the Office finds a non-compliance with this Act or special regulation[2]), the Office shall not permit the certification body to issue or renew a certificate and shall issue a decision in that respect.

(8) There is no appeal against the decision on permission issuing certificate or decision on permission renewing certificate by the certification body.

(9) Appeal may be submitted against decision on non-permission issuing certificate or decision on non-permission renewing certificate by certification body, and such appeal shall be decided by the president of the Office.

(10) Within 15 days from certificate issuance, renewal or revoking, the certification body shall inform the Office of

a) its identifying information;

b) number of the declaration issued to that body;

c) identifying information of the relevant controller or processor;

d) subject-matter of the certificate;

e) certificate number;

f) reasons for certificate issue, renewal or withdrawal.

(11) A certificate issued by a certification body shall particularly contain

a) identifying information of a certification body including the number of declaration on granting accreditation;

b) applicant's identifying information;

c) subject-matter of the certificate;

d) certification criteria based on which the certificate is being issued;

e) certificate number;

f) certificate issue date; or, where certificate renewal is concerned, also the date of the previous issue of the certificate;

g) imprint of the official seal of the certification body and signature of the person authorised to act on behalf of the certification body stating his or her name and surname.

(12) The certification body shall

a) meet the requirements laid down under this Act and the accreditation criteria in accordance with accreditation granting decision;

b) no later than in 15 days, notify the Office in writing of any changes to the accreditation granted;

c) allow the Office to exercise supervision pursuant to this Act;

d) adhere to the principle of independence;

e) archive documentation relating to the compliance with the certification process under special regulation.[41])

TITLE III

INSPECTION

Section 90
Initiating an inspection

(1) Inspection of personal data processing, inspection of adherence to the code of conduct approved by the Office pursuant to section 85, inspection of compliance of personal data processing with the issued certificate pursuant to section 86, and inspection of adherence of the issued declaration of granting accreditation pursuant to section 87 and section 88 (hereafter as "inspections") are executed by the Office through an inspection body composed of employees of the Office (hereafter as "Inspection body").

(2) Each member of the Inspection body executes inspection based on a written mandate of the leading employee; if the leading employee is a member of the Inspection body, members of Inspection body execute the inspection based on the written mandate of the president of the Office.

(3) Member of the Inspection body shall be employee of the Office with integrity, has a relevant professional education and experience in the field forming part of the Office´s inspection activities.

(4) Written mandate to carry out an inspection shall contain

a) identifying information of the Office,

b) identifying information of the inspected person,

c) the academic degree, name and surname of the Inspection body member who will execute the inspection,

d) imprint of an official stamp and signature.

(5) The Office shall publish a template of the mandate to execute inspection on its website.

(6) An inspection is initiated on the day when the inspection notification is delivered to the controller or processor or their representatives if he had been appointed, or to the monitoring body pursuant to section 87 or certification body pursuant to section 88 (hereafter as "inspected person").

(7) The Inspection body shall execute the inspection based on an inspection plan or based on the suspicion of a breach of the obligation in the course of personal data processing pursuant to this Act or special regulations[2)] or in the course of personal data protection proceeding.

(8) When executing inspection, the Inspection body shall act in such a way that the rights and legally protected interests of the inspected person are not affected.

Section 91
Inspection body's bias

(1) A member of the Inspection body who has become aware of facts which could establish doubts about his or her bias or bias of another member of the Inspection body shall notify in writing without undue delay whoever mandated him or her pursuant to section 90 paragraph 2 about such circumstances.

(2) If an inspected person has any doubts about the bias of Inspection body or its member regarding his or her relationship to the subject matter of the inspection or to inspected person, he or she is entitled to submit written objections with justification within 15 days from the day he or she became aware about such circumstances. The submitting of the objections does not have a suspensive effect; the Inspection body is empowered, pursuant to the first sentence, to carry out in respect of inspection only such actions that cannot be delayed.

(3) Any objections from an inspected person regarding bias and notification about bias of the Inspection body member shall be decided by the entity that has mandated the Inspection body pursuant to section 90 paragraph 2 within ten working days from raising them and written form of decision shall be delivered to whom the objection was raised. The appeal against decision on objections of bias and against the decision on notification about the bias of an Inspection body member cannot be submitted.

Section 92
Obligations of the Inspection body

The Inspection body shall

a) provide prior writing notification to the inspected person about the subject matter of the inspection; if the notification of the inspection before the beginning of execution of the inspection could lead to frustrate of the purpose of inspection or significant obstruction of the inspection execution, the Inspection body may notify the subject matter of inspection immediately prior to executing of inspection,

b) notify in writing about the date and time of the execution of inspection in the period of a minimum ten days prior to executing inspection; if the notification of the beginning of execution of the inspection could lead to frustrate of the purpose of inspection or significant obstruction of the inspection, the Inspection body may notify the beginning of execution of the inspection immediately prior to executing of inspection,

c) before the beginning of execution of the inspection and at any time upon request of the inspected person, show the mandate to execute the inspection and service card,

d) elaborate the minutes of the executing of the inspection minutes,

e) elaborate an inspection protocol with inspection findings (hereafter as "protocol") or an inspection report,

f) provide inspected person' statements pursuant to point a) of section 95 in the inspection protocol or inspection report,

g) elaborate minutes on giving an explanation pursuant to point j) of section 93 and point e) of section 94,

h) deliver one copy of the minutes of the execution of the inspection, minutes on giving an explanation, and the inspection protocol or inspection report to the inspected person,

i) confirm to the inspected person in writing the receipt of the original documents or copies of documents, written documentation, copies of storage media and other materials and evidence and ensure their protection against their loss, destruction, damage or their abuse,

j) review the justification of the objections to the inspection findings listed in the protocol and consider the justification of the objection in an annex to the protocol and inform the inspected person,

k) discuss the protocol with the inspected person and elaborate minutes on this discussion.

Section 93
Rights of Inspection body

The Inspection body has the right to

a) enter the land and premises of an inspected person, if there is no need for permission pursuant to a special regulation,[33)]

b) have access to means and devices that serve, could serve or should serve for personal data processing by the inspected person,

c) have access to data in automated processing devices up to the level of system administrator, including that in the scope needed for executing the inspection,

d) verify the identity of natural persons that act on behalf of the inspected person or cooperate with the Inspection body,

e) require from the inspected person to provide the Inspection body with originals or copies of documentation, other documents, statements and information, personal data processed on storage media, including technical storage media for personal data, printouts and source codes of programmes if he or she owns them or are available to them in compliance with the conditions to their acquisition, and other materials or documents needed for the inspection; in justified cases allowing the Inspection body to take originals or copies even outside the premises of the inspected person,

f) request from the inspected person within a reasonable time complete and correct oral and written information, statements and explanations of inspected facts and facts related to the inspection,

g) document evidence related to the inspection by making pictures, audio recordings, video recordings or audio-video recordings, even without the data subject's consent,

h) request the inspected person's cooperation in other areas falling under the scope of the subject matter of the inspection,

i) require cooperation at the place of inspection from others than the inspected person,

particularly from the inspected person's processor and his employees or other persons if it is reasonable to presume that their activities are related to the subject matter of inspection or if it is deemed necessary for clarification of facts related to the subject matter of inspection,

j) summons the inspected person and others than the inspected person to appear in the determined time and in the determined place with the aim to provide the explanation relating to the subject matter of inspection,

k) perform joint operations together with supervisory authorities of other member states pursuant to a special regulation.[44)]

Section 94
Obligations of inspected person

The inspected person shall

a) tolerate the execution of the inspection and create adequate conditions for the Inspection body for executing the inspection and processing inspection findings,

b) cooperate with the Inspection body which is essential for proper execution of inspection, particularly in documenting an adequate level of security with a view to risks represented by personal data processing in the condition of the controller and processor,

c) at the time of execution of the inspection to ensure for the Inspection body accessibly and safety access to devices, means and filling systems,

d) provide to the Inspection body required cooperation in accordance with its rights as defined by section 93 and refrain from acting that could frustrate the execution of inspection,

e) present himself or herself at the request of the Inspection body with the aim to provide explanation relating to the subject matter of the inspection,

f) provide to Inspection body originals or copies of documentation, other documents, statements and information, personal data processed on memory media, including technical personal data storage media, printouts and source codes of programmes within determined period if he or she owns them or are available to them, and further materials necessary for the inspection and in reasonable cases allowing to take the originals or copies of documents even outside the premises of the inspected person,

g) provide to the Inspection body complete and correct oral and written information, statements and explanations to the inspected facts and to the facts related to the inspection,

h) present himself or herself at the request of the Inspection body to discuss the protocol.

Section 95
Rights of inspected person

The inspected person has the right to

a) comment the facts identified throughout the inspection at the ongoing basis,

b) become aware with the content of protocol and submit written objections to findings after becoming aware of inspection findings mentioned in the protocol,

c) request from the Inspection body to demonstrate facts pursuant to point b) and c) of section

92,

d) request from invited person to show a written mandate of the president of the Office pursuant to section 96 paragraph 2,

e) request from the Inspection body confirmation of withdraw of originals of documentation or copies of documentation pursuant to point c) of section 93.

Section 96
Invited person

(1) The Inspection body may invite another natural person or representative of another supervisory authority of the Member State to perform inspection (hereafter as "invited person") if it is reasonable by the special character of the inspection. Participation of an invited person in executing the inspection is considered as another act in general interest.

(2) The invited person participates in the inspection based on written mandate by the president of the Office; the Inspection body notify the inspected person about the invitation pursuant to point a) of section 92.

(3) The invited person shall demonstrate his or her authorisation for performing the inspection to the inspected person by a written mandate to execute the inspection pursuant to section 90 paragraph 2 and point c) of section 92, no later than at the beginning of the execution of the inspection.

(4) The invited person shall keep the secrecy on facts he or she has known during the inspection even after the inspection has been completed. The president of the Office may acquit of the invited person's obligation of secrecy. A representative of another supervisory authority of the Member State as an invited person is not bound by the obligation of secrecy towards the seconding supervisory authority of the Member State in the scope necessary for completing tasks related to participation in the inspection.

(5) The invited person may not perform the tasks pursuant to this Act or special regulation[2]) if in consideration of its relationship with the subject matter of the inspection or inspection person its impartiality may be questionable. An invited person that has knowledge about facts that could establish doubts about its impartiality shall notify the president of the Office about such facts without undue delay.

(6) The inspected person may raise substantiated objections on the bias of the invited person in writing. An invited person may perform only such actions which cannot be postponed within the framework of the inspection until the decision on the objections of the bias is issued.

(7) The president of the Office shall decide about notification on bias of invited person pursuant to paragraph 5 and about objection on bias of inspected person pursuant to paragraph 6 within ten working days of their delivery. The president of Office decision cannot be appealed.

Section 97
Termination of the inspection

(1) The outcome of the inspection is an inspection protocol or inspection report.

(2) If the inspection identified any shortcomings in personal data processing, the Inspection body shall elaborate the inspection protocol containing the following:

a) identifying information of the Office,

b) identifying information of the inspected person,

c) the date of initiation of the inspection,

d) the subject matter of the inspection,

e) the demonstrated findings of the inspection including their justification,

f) the academic degree, name and surname of the Inspection body member who performed the inspection,

g) protocol elaboration date,

h) imprint of the Office's official stamp and signatures of the Inspection body members.

(3) If the inspection protocol pursuant to paragraph 2 contains annexes demonstrating findings of inspection, they form part of the inspection protocol.

(4) The inspected person has the right to submit written objections after he or she becomes known with the findings of inspection within 21 days from the day the protocol was delivered. Objections submitted after this period shall not be considered by Inspection body.

(5) If objections are filed against the findings of inspection pursuant to paragraph 4 or if new circumstances relating to the subject matter of the inspection are identified, the Inspection body shall review whether they are substantive and elaborates an annex which is an integral part of protocol. If the Inspection body does not accept the inspected person's objections, shall justify it in annex; the annex shall be elaborated accordingly to paragraph 2.

(6) The Inspection body shall inform the inspected person in writing about the results of the review of the objections within 15 working days from the day when the objections are delivered.

(7) The Inspection body shall invite the inspected person in writing to discuss the inspection protocol after the results of the review of the objections have been delivered to the inspected person pursuant to paragraph 6, or after the period to submit objection by inspected person pursuant to paragraph 4 has expired; the Inspection body shall elaborate minutes on the discussion of the protocol, which is a part of the protocol.

(8) If the inspection does not identify any breaches of obligations lay down by this Act or special regulations,[2)] the Inspection body shall elaborate an inspection report. When elaborating such a report, it shall proceed in compliance with paragraphs 2 and 3.

(9) The inspection shall be terminated

a) on the day when the minutes on discussing the protocol are signed,

b) on the day of refusal to sign the minutes on discussing the protocol, about which the Inspection body elaborate a report in the minutes on discussing the protocol,

c) on the day when the inspected person failed to present himself or herself for the purposes of discussing the protocol upon the Inspection body's written request pursuant to paragraph 7, which the Inspection body elaborate a report in the minutes on discussing the protocol, or

d) on the day of delivering the inspection report pursuant to paragraph 8.

Section 98

A special regulation[45)] does not apply to execution of the inspection.

TITLE IV

PERSONAL DATA PROTECTION PROCEEDING

Section 99
Personal data protection proceeding

(1) The purpose of personal data protection proceeding (hereafter as "proceeding") is to determine whether there was any infringement of the rights of natural persons when their personal data were processed or if there was any violation to this Act or a special regulation[2)] in the area of personal data protection; and, if any deficiencies are identified, if it is reasonable and useful, to impose corrective measures or impose a fine for violation of this Act or a special regulation[2)] for the area of personal data protection.

(2) The proceeding is not public.

(3) Parties to the proceeding may be

a) a data subject that has lodged a complaint to initiate proceeding pursuant to section 100,

b) a controller,

c) a processor,

d) a certification body,

e) a monitoring body.

(4) If the data subject's complaint pursuant to section 100 concerns the controller or the processor, for which the competent supervisory authority is the main establishment or the one establishment of the controller or processor for cross-border processing performed by the controller or processor pursuant to a special regulation (hereafter as „lead supervisory authority"),[46)] the Office proceeds pursuant to a special regulation.[47)]

(5) The Office shall inform the data subject about the decision of the lead supervisory authority. If the lead supervisory authority decides to reject or dismisses or will not act on the complaint pursuant to a special regulation,[47)] the Office shall initiate proceedings pursuant to section 100.

(6) If personal data processing pursuant to paragraph 4 is relevant to the controller or processor that processes personal data on a legal basis pursuant to point c) or e) of paragraph 1 section 13, the Office is materially competent and the procedure pursuant to paragraph 4 does not apply.

Section 100
Initiation of proceeding

(1) Proceeding is initiated based on the complaint of a data subject that claims that his or her rights lay down by this Act are directly influenced (hereafter as "the complainant"), or without a complaint.

(2) The Office shall initiate proceedings without a complaint upon its findings during the carried out of supervision over the compliance with obligations lay down by this Act or a special regulation.[2)]

(3) A complaint to initiate proceeding pursuant to paragraph 1 (hereafter as "complaint") shall contain:

a) the name, surname, correspondence address and signature of the complainant,

b) identification of the entity against which the complaint is addressed, with name, surname, permanent residency or organisation name, headquarter and identification number if such number was assigned,

c) the subject of the complaint, identifying the rights that might have been infringed during personal data processing,

d) evidence supporting the arguments lay down by the complaint,

e) a copy of document or other type of evidence demonstrating the exercise of a right pursuant to second title of second chapter of this Act or special regulations,[2)] if such right has been exercised by the data subject, or justification of special consideration if such right has not been exercised by the data subject, if the complaint was lodged by a data subject.

(4) The Office shall publish a template of complaint at its website.

(5) The Office shall postpone the complaint if

a) the complaint is manifestly unfounded,

b) the subject of the complaint is reviewed by a court or law enforcement authority,

c) the complainant has not provided necessary cooperation upon the Office's request, while without his or her active participation the complaint cannot be resolved; the Office shall notify the complainant about the possibility of postponing the complaint,

d) more than three years have passed from the event that is subject of the complaint as of the day when the complaint was delivered.

(6) If the complaint does not include a request to keep the identity of the complainant confidential, the Office shall resolve the complaint without preserving the confidentiality of the personal data in the complaint. If the complaint includes a request for keeping the identity of the complainant confidential, but the character of the complaint does not allow the processing of such complaint without indicating some of the complainant's personal data, the Office upon identifying such circumstances shall notify the complainant, that it will continue processing with the complaint only provided that the complainant consent is to be given identifying information about his or her personal data for the purposes of processing the complaint within a specified period.

(7) If the complaint is delivered to the Office by a person other than the data subject, the complaint is considered as a petition to initiate proceedings without a complaint (hereafter as "petition").

(8) The Office shall review the petition within 30 days from the date it is delivered to the Office, and if it does not postpone the petition pursuant to paragraph 5, shall initiate proceeding and shall decide on the merits of the case pursuant to section 102.

(9) The complainant shall be notified about how the petition is processed pursuant to paragraph 8 within 30 days from the date the petition is delivered by the Office.

Section 101
Periods

(1) The Office shall decide in the proceeding within 90 days from the day proceeding is initiated. In the reasonable cases this period is extended by Office, to a maximum of 180 days. The Office notifies the parties of the proceeding about the extension in writing.

(2) If it is necessary to carry out an inspection during the proceeding, the period for issuing a decision pursuant to paragraph 1 does not run, from the day of the inspection is initiated until the inspection is finalised.

(3) If the Office knows that the conditions were met for suspension of the proceedings pursuant to a special regulation,[48)] the Office shall suspend the proceedings and inform the parties thereof.

Section 102
Decision

(1) If the Office identifies that rights of data subject were infringed or failure to comply with obligations when processing personal data lay down by this Act or special regulations[2)] in personal data processing by the party to proceeding, it can by decision to

a) impose corrective measures and a period within which the measures pursuant to paragraph 3 shall be carried out, if reasonable and useful,

b) cancel the binding character of the approved Code of Conduct for the controller or processor who have committed themselves to comply with such Code of Conduct,

c) withdraw a certificate,

d) order the certification body to withdraw a certificate,

e) withdraw a declaration on granting accreditation,

f) impose a fine pursuant to section 104.

(2) If the Office does not decide in proceeding pursuant to paragraph 1, and if the infringement of rights of the data subject was not proven or if the obligations lay down by this Act or special regulation related to personal data processing are not proven to have failed[2)] by the party to the proceeding, the Office shall suspend the proceedings.

(3) The Office may impose an obligation to the controller or processor, particularly order

a) to eliminate identified deficiencies and the reducing the causes contributing to it within a period lay down by the Office,

b) to adopt technical and organisational measures to ensure a level of security appropriate to the risks to the rights of natural persons,

c) to assess the impact of processing operations for the purposes of personal data protection in compliance with this Act or a special regulation.[2)]

(4) If violation of the data subject's rights or of obligations in personal data processing cannot be postponed, the Office shall adopt a provisional measure.

(5) The controller or processor shall inform the Office in writing about complying with measures imposed by the Office within the period lay down by the Office.

Section 103

(1) A decision adopted pursuant to section 102 may be appealed, which decided by the president of the Office.

(2) The appealing party may extend the scope of the submitted appeal by an additional proposal or other points only within the period lay down for filing the appeal.

TITLE V

ADMINISTRATIVE OFFENCES

Section 104

(1) The Office may impose a fine of up to €10 000 000 or in case of an undertaking turnover is up to 2% of total annual turnover worldwide for the previous accounting year depending on which amount is higher, to:

a) a controller, including a public authority and a public institution, for failing or breaching any of the obligations lay down by section 15, section 18, sections 31 to 35, section 37, sections 39 to 45, sections 79 and section 109 or pursuant to article 8, article 11, articles 25 to 39, article 42 and article 43 of the Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation) (OJ EU L 119, 4. 5. 2016) (hereafter as "Regulation (EU) 2016/679"),

b) a competent authority for failing to comply with or for breaching some of the obligations under sections 67 to 72,

c) a processor, including a public authority and a public institution in the position of processor, for failing or breaching any of the obligations lay down by sections 34 to 37, section 39, section 40 paragraph 3, section 44, section 45, section 69 paragraph 3, section 71, section 79 and section 109, or pursuant to articles 27 to 33, articles 37 to 39, article 42 and article 43 of Regulation (EU) 2016/679,

d) a certification body for failing or breaching any of the obligations lay down by sections 88 and 89 or pursuant to articles 42 and 43 of Regulation (EU) 2016/679,

e) a monitoring body for failing or breaching any of the obligations lay down by section 87 paragraphs 5 and 19 or pursuant to article 41 paragraph 4 of Regulation (EU) 2016/679.

(2) The Office may impose a fine up to €20 000 000 or in case of an undertaking up to 4% of the total annual global turnover for the previous accounting year depending on which amount is higher, to who

a) has not complied with or breached any of the fundamental principles of personal data processing, including the obligation to obtain consent pursuant to sections 6 to 14, section 16 and sections 52 to 58 or pursuant to articles 5 to 7 and article 9 of the Regulation (EU) 2016/679,

b) has not complied with or infringed some of the rights of a data subject pursuant to sections 19 to 29 and sections 59 to 66 or pursuant to articles 12 to 22 of Regulation (EU) 2016/679,

c) has not complied with or has breached any of the obligations in personal data transfer to a third-country recipient or international organisation pursuant to sections 49 to 51 and sections 73 to 77 or pursuant to articles 44 to 49 of Regulation (EU) 2016/679,

d) has not complied with or has breached any of the obligations related to lawful processing of personal data pursuant to section 78,

e) has not complied with an order on personal data processing or has not complied with temporary or permanent limitations to personal data processing or suspension of transfer of personal data as ordered by the Office pursuant to section 81 paragraph 3 or to article 58 paragraph 2 of Regulation (EU) 2016/679 or has not provided access in contradiction with article 58 paragraph 1 of Regulation (EU) 2016/679.

(3) The Office may impose a fine of up to €20 000 000 to an entity that has not complied with a measure imposed by the Office pursuant to point a) of section 102 paragraph 1 or article 58 paragraph 2 of Regulation (EU) 2016/679 or in case of an undertaking up to 4% of the total annual global turnover for the previous accounting year depending on which amount is higher.

Section 105

(1) The Office may also impose an administrative fine up to €2 000 to a person that is not a controller or processor for not providing requested cooperation to the Office when performing the supervision pursuant to section 109 or a special regulation.[2)]

(2) The Office may also impose an administrative fine to the controller or processor, or representative of controller or processor

a) up to €2 000 if it does not ensure adequate conditions for performing an inspection pursuant to point a) of section 94,

b) up to €10 000 if it obstructs the performance of an inspection pursuant to points b) to h) of section 94.

Section 106

(1) The Office imposes fines and administrative fines depending on the individual circumstances of a given case. When deciding about imposing a fine and the level of the fine pursuant to section 104, the Office considers in particular:

a) the nature, severity, and duration of the breach, nature, scope or purpose of personal data processing, as well as the number of data subjects affected, and scope of damage if applicable,

b) possible guilty for breaching of personal data protection,

c) measures that the controller or processor had adopted to mitigate damages suffered by data subjects,

d) the level of accountability of the controller or processor with consideration to technical and organisational measures adopted pursuant to section 32, sections 39 and 42,

e) previous breaches of the personal data protection by the controller or processor,

f) the level of cooperation with the Office in correcting to breach of personal data protection and mitigation of potential negative consequences of such breach,

g) the category of personal data to which the breach relates,

h) the manner in which the Office known about the personal data protection breach, particularly if the controller or processor reported the breach and if so to which extent,

i) compliance with measures imposed earlier in the proceeding pursuant to section 102 paragraph 1, if applicable, by the controller or processor,

j) compliance with approved Codes of Conduct pursuant to section 85 or issued certificates pursuant to section 86,

k) aggravating or alleviating circumstances, particularly financial benefits or losses that have been prevented directly or indirectly in connection with branch of the personal data protection.

(2) If the controller or processor intentionally or out of negligence infringed, by the same processing operations or related processing operations, various provisions of this Act or special regulation,[2)] the total amount of the fine may not exceed the level lay down for the most serious personal data protection breaches pursuant to section 104.

(3) A fine pursuant to section 104 may be imposed within two years from the day when the Office identified the infringement of the obligation, but no later than five years from the day when the infringement occurred.

(4) An administrative fine pursuant to section 105 may be imposed by the Office repeatedly if obligation was not complied within the defined period.

(5) An administrative fine pursuant to section 105 may be imposed within six months from the day when the infringement of obligation occurred.

(6) Fines and administrative fines are represented state budget incomes.

CHAPTER SIX

COMMON, TRANSITIONAL AND FINAL PROVISIONS

Section 107
Common provisions

(1) Proceedings pursuant to this Act are governed by the Code of Administrative Procedure, unless otherwise provided for by paragraph 2.

(2) The Code of Administrative Procedure shall not be applied to decisions on Inspection body bias pursuant to section 91, to decisions on the bias of invited persons pursuant to section 96 paragraphs 5 to 7 and to inspection pursuant to third title of chapter five, with the exception of delivering written documents during carried out of the inspection.

Section 108

(1) The Office shall issue legislative act of general application to implement section 29 paragraph 9, section 70 paragraph 4, section 86 paragraph 19, section 87 paragraph 20 and section 88 paragraph 19.

(2) Further cases of processing operations that are subject to data protection impact assessment and the procedure in data protection impact assessment pursuant to this Act shall be lay down by a legislative act of general application issued by the Office.

Section 109
Cooperation

Anyone shall cooperate with the Office as it performs its duties and competencies and allow the Office to supervise whether the obligations lay down by this Act or special provision[2)] and decisions issued based on this Act. This provision does not apply to section 81 paragraphs 7 and 8.

Section 110
Transitional provisions

(1) The Office for Personal Data Protection of the Slovak Republic pursuant to the previous Act is the Office pursuant to this Act and a supervisory Authority pursuant to special regulation.[2)]

(2) The president of the Office for Personal Data Protection of the Slovak Republic elected to the position pursuant to the previous Act is president of the Office pursuant to this Act, and his or her term of office is not influenced thereby.

(3) The vice-president of the Office for Personal Data Protection of the Slovak Republic appointed to the position pursuant to the previous law is vice-president pursuant to this Act, and his or her term of office is not influenced thereby.

(4) The Head Inspector of the Office, appointed to the position pursuant to the previous Act, shall terminate his or her function as of the date when this Act enters into force.

(5) If the Head Inspector of the Office, who finished performing duties arising from this position pursuant to paragraph 4, and who was a state employee in permanent service pursuant to a special regulation,[7)] that person is considered a state employee in permanent civil service pursuant to a special regulation from the day when this Act entered into force.[7)] If the Head Inspector of the Office whose function terminated pursuant to paragraph 4 was a state employee in temporary civil service pursuant to a special regulation,[7)] his or her employment in state service shall be terminated as of the date when this Act enters into force.

(6) The term of office of an inspector of the Office who was appointed to the position pursuant to the previous law shall terminate as of the date when this Act enters into force.

(7) The inspector of the Office whose term of office terminated pursuant to paragraph 6 is considered, from the date when this Act entered into force, for a civil servant pursuant to a special regulation.[7)]

(8) An inspection initiated pursuant to the previous Act shall be completed pursuant to that Act.

(9) Personal data protection proceeding pursuant to the previous Act and fines proceeding pursuant to the previous Act, initiated but not legally terminated by 24 May 2018, shall be completed pursuant to the previous Act.

(10) The competent authority shall provide for keeping logs pursuant to section 69 in information systems of personal data established pursuant to the previous regulations until 6 May 2023; if this would cause serious problems for the functioning of a given operating

system of personal data, then the competent authority shall guarantee that logs shall be kept pursuant to section 69 of 6 May 2026 at the latest.

(11) Consent to personal data processing given pursuant to the previous Act that is in compliance with this Act or a special regulation,[2)] is considered consent to personal data processing pursuant to regulations forced of 25 May 2018.

(12) A data protection officer pursuant to the previous Act, who meets the requirements lay down by this Act or a special regulation,[2)] is considered a data protection officer pursuant to regulations forced of 25 May 2018.

Section 111

This Act transposes legally binding act of the European Union listed in the Annex.

Section 112
Repeal provision

This Act repeals:

1. Act No. 122/2013 on Personal Data Protection as amended and in the wording of Act No. 84/2014,

2. Decree of the Office for Personal Data Protection of the Slovak Republic No. 164/2013 on the Scale and Documentation of Security Measures in the wording of decree No. 117/2014,

3. Decree of the Office for Personal Data Protection of the Slovak Republic No. 165/2013 that lays down details on the examination of a natural person for the position of data protection officer.

Article II

Act No. 124/1992 on Military Police in the wording of Act No. 422/2002, of Act No. 240/2005, of Act No. 393/2008, of Act No. 491/2008, of Act No. 192/2011, of Act No. 220/2011, of Act No. 313/2011 and Act No. 96/2012 is amended as follows:

1. In section 35b, paragraph 6 is deleted.

   Current paragraphs 7 to 9 are marked as paragraphs 6 to 8.

2. In section 35c, paragraph 4 is deleted.

   Current paragraphs 5 and 6 are marked as paragraphs 4 and 5.

3. In section 35c paragraph 5 the words “of paragraphs 1 to 4” are replaced by the words “of paragraphs 1 to 3”.

4. In section 35gb the paragraphs 1 and 2 are deleted.

   Current paragraphs 3 to 8 are marked as paragraphs 1 to 6.

5. In section 35gb paragraph 3 the words “section 35gd paragraph 3” are replaced by the words “section 35ga paragraph 3”.

6. In section 35gb paragraph 6 the words “section 35b paragraph 8 and 9” are replaced by the words “section 35b paragraph 7 and 8“.

7. In section 35gc the paragraphs 3 to 5 are deleted.

8. In section 35gd the paragraphs 1 to 3 and 5 to 11 are deleted, including the footnotes to references 5l, 5m and 5n.

   Further, the identification of paragraph 4 is deleted.

9. Section 35ge is deleted.

Article III

Act of the National Council of Slovak Republic No. 171/1993 on the Police Force in the wording of Act of the National Council of Slovak Republic No. 251/1994, of Act of the National Council of Slovak Republic No. 233/1995, of Act of the National Council of Slovak Republic No. 315/1996, Act No. 353/1997, Act No. 12/1998, Act No. 73/1998, Act No. 256/1998, Act No. 116/2000, Act No. 323/2000, Act No. 367/2000, Act No. 490/2001, Act No. 48/2002, Act No. 182/2002, Act No. 422/2002, Act No. 155/2003, Act No. 166/2003, Act No. 458/2003, Act No. 537/2004, Act No. 69/2005, Act No. 534/2005, Act No. 558/2005, Act No. 255/2006, Act No. 25/2007, Act No. 247/2007, Act No. 342/2007 , Act No. 86/2008, Act No. 297/2008, Act No. 491/2008, Act No. 214/2009, Finding of the Constitutional Court of the Slovak Republic No. 290/2009, Act No. 291/2009, Act No. 495/2009, Act No. 594/2009, Act No. 547/2010, Act No. 192/2011, Act No. 345/2012, Act No. 75/2013, Act No. 307/2014, Finding of the Constitutional Court of the Slovak Republic No. 139/2015, of Act No. 397/2015, of Act No. 444/2015, of Act No. 125/2016 and of Act No. 82/2017 is amended as follows:

1. In section 69, paragraphs 5, 7 and 8 are deleted.

   Current paragraphs 6 and 9 to 16 are marked as paragraphs 5 to 13.

2. In section 69a paragraph 1 the following words “including protection against threats to public safety and prevention of such threats” are inserted behind the word “proceedings”.

3. In section 69a paragraph 3, the words “personal data that identify race or ethnic origin, political opinions, religion or faith, membership in political parties or political movements, membership in trade union organisations and data on health and sexual life (hereafter as “special categories of personal data”) are replaced by the words “special categories of personal data[28l])”.

   The footnote to reference 28l reads as follows:

   “[28l]) Act No. 18/2018 on personal data protection and amending and supplementing certain Acts.”

4. In section 69a, paragraphs 4 and 6 are deleted.

   Current paragraphs 5 and 7 are marked as paragraphs 4 and 5.

5. In section 69a paragraph 5, in the first and second sentence the words “of paragraphs 1 and 6” are replaced with the words “of paragraph 1”.

6. Section 69c including the title reads as follows:

“Section 69c

Sharing information about personal data

(1) The Police Force is authorised to request a party that has provided or made accessible personal data pursuant to a special regulation not, without prior consent of the Police Force, to inform a data subject about processing of provided personal data or data that were made accessible.

(2) If the Police Force is asked to provide information on personal data pursuant to a special regulation and the personal data were provided or made accessible to authorities of another EU member state (hereafter as “member state authority”) authorised to prevent and discover criminal activities, identify perpetrators of criminal activities, investigate crimes or execute decisions in criminal proceedings, including protecting against and preventing threats to public safety, or from another authority of a member state under the condition not to inform the data subject about personal data processing without its prior consent, the Police Force shall provide the data subject information on personal data processing only with the prior consent of the member state authority that has provided or made accessible such personal data.

(3) The Police Force is authorised to process copies of documentation provided to the Police Force by the data subject when exercising his or her rights pursuant to a special regulation.”

Footnote to reference 27da is deleted.

7. Section 69f is deleted.

Article IV

Act of the National Council of Slovak Republic No. 145/1995 on Administrative Fees as amended by Act of the National Council of Slovak Republic No. 123/1996 and Act of the National Council of Slovak Republic No. 224/1996, Act No. 70/1997, Act No. 1/1998, Act No. 232/1999, Act No. 3/2000, Act No. 142/2000, Act No. 211/2000, Act No. 468/2000, Act No. 553/2001, Act No. 96/2002, Act No. 118/2002, Act No. 215/2002, Act No. 237/2002, Act No. 418/2002, Act No. 457/2002, Act No. 465/2002, Act No. 477/2002, Act No. 480/2002, Act No. 190/2003, Act No. 217/2003, Act No. 245/2003, Act No. 450/2003, Act No. 469/2003, Act No. 583/2003, Act No. 5/2004, Act No. 199/2004, Act No. 204/2004, Act No. 347/2004, Act No. 382/2004, Act No. 434/2004, Act No. 533/2004, Act No. 541/2004, Act No. 572/2004, Act No. 578/2004, Act No. 581/2004, Act No. 633/2004, Act No. 653/2004, Act No. 656/2004, Act No. 725/2004, Act No. 725/2004, Act No. 5/2005, Act No. 8/2005, Act No. 15/2005, Act No. 93/2005, Act No. 171/2005, Act No. 308/2005, Act No. 331/2005, Act No. 341/2005, Act No. 342/2005, Act No. 468/2005, Act No. 473/2005, Act No. 491/2005, Act No. 538/2005, Act No. 558/2005, Act No. 572/2005, Act No. 573/2005, Act No. 610/2005, Act No. 14/2006, Act No. 15/2006, Act No. 24/2006, Act No. 117/2006, Act No. 124/2006, Act No. 126/2006, Act No. 224/2006, Act No. 342/2006, Act No. 672/2006, Act No. 693/2006, Act No. 21/2007, Act No. 43/2007, Z. z., Act No. 95/2007, Act No. 193/2007, Act No. 220/2007, Act No. 279/2007, Act No. 295/2007, Act No. 309/2007, Act No. 342/2007, Act No. 342/2007, Act No. 343/2007, Act No. 344/2007, Act No. 355/2007, Act No. 358/2007, Act No. 359/2007, Act No. 460/2007, Act No. 517/2007, Act No. 537/2007, Act No. 548/2007, Act No. 571/2007, Act No. 577/2007, Act No. 647/2007, Act No. 661/2007, Act No. 92/2008, Act No. 112/2008, Act No. 167/2008, Act No. 214/2008, Act No. 264/2008, Act No. 405/2008, Act No. 408/2008, Act No. 451/2008, Act No. 465/2008, Act No. 495/2008, Act No. 514/2008, Act No. 8/2009, Act No. 45/2009, Act No. 188/2009, Act No. 191/2009, Act No. 274/2009, Act No. 292/2009,

Act No. 304/2009, Act No. 305/2009, Act No. 307/2009, Act No. 465/2009, Act No. 478/2009, Act No. 513/2009, Act No. 568/2009, Act No. 570/2009, Act No. 594/2009, Act No. 67/2010, Act No. 92/2010, Act No. 136/2010, Act No. 144/2010, Act No. 144/2010, Act No. 514/2010, Act No. 556/2010, Act No. 39/2011, Act No. 119/2011, Act No. 200/2011, Act No. 223/2011, Act No. 254/2011, Act No. 256/2011, Act No. 258/2011, Act No. 324/2011, Act No. 342/2011, Act No. 363/2011, Act No. 381/2011, Act No. 392/2011, Act No. 404/2011, Act No. 405/2011, Act No. 409/2011, Act No. 519/2011, Act No. 547/2011, Act No. 49/2012, Act No. 96/2012, Act No. 251/2012, Act No. 286/2012, Act No. 336/2012, Act No. 339/2012, Act No. 351/2012, Act No. 439/2012, Act No. 447/2012, Act No. 459/2012, Act No. 8/2013, Act No. 39/2013, Act No. 40/2013, Act No. 72/2013, Act No. 75/2013, Act No. 94/2013, Act No. 96/2013, Act No. 122/2013, Act No. 144/2013, Act No. 154/2013, Act No. 213/2013, Act No. 311/2013, Act No. 319/2013, Act No. 347/2013, Act No. 387/2013, Act No. 388/2013, Act No. 474/2013, Act No. 506/2013, Act No. 35/2014, Act No. 58/2014, Act No. 84/2014, Act No. 152/2014, Act No. 162/2014, Act No. 182/2014, Act No. 204/2014, Act No. 262/2014, Act No. 293/2014, Act No. 335/2014, Act No. 399/2014, Act No. 40/2015, Act No. 79/2015, Act No. 120/2015, Act No. 128/2015, Act No. 129/2015, Act No. 247/2015, Act No. 253/2015, Act No. 259/2015, Act No. 262/2015, Act No. 273/2015, Act No. 387/2015, Act No. 403/2015, Act No. 125/2016, Act No. 272/2016, Act No. 342/2016, Act No. 386/2016, Act No. 51/2017, Act No. 238/2017, Act No. 242/2017, Act No. 276/2017, Act No. 292/2017, Act No. 293/2017, Act No. 336/2017 and Act No. 17/2018 is amended as follows:

In the List of Administrative Fees, part XXIII. PERSONAL DATA PROTECTION, item 273 is defined as follows:

“Item 273

a) Proceedings on approved a code of conduct.....€1,000

b) Proceedings on amendments to a Code of Conduct..... €1,000

c) Proceedings on extending a code of conduct..... €1,000

d) Proceedings on issued a certificate..... €5,000

e) Proceedings on certificate renewal..... €5,000

f) Proceedings on granting accreditation €7,000

g) Proceedings on authorisation of a certification body..... €250“.

Article V

Act No. 4/2001 on Corps of Prison and Court Guard in the wording of Act No. 422/2002, of Act No. 166/2003, of Act No. 537/2004, of Act No. 581/2004, of Act No. 475/2005, of Act No. 491/2008, of Act No. 59/2009, of Act No. 192/2011, of Act No. 220/2011, of Act No. 372/2013, of Act No. 307/2014, of Act No. 176/2015, of Act No. 386/2015, of Act No. 444/2015, of Act No. 125/2016 of Act No. 255/2016 is amended as follows:

1. Section 65b including the title reads as follows:

“Section 65b

Control, rectification and erasure of information or personal data

(1) If the circumstances permit, Corps of Prison and Court Guard shall, when the personal data is provided, assess whether the data is correct and if needed shall add available information, that shall allow assess of the correctness of the data.

(2) If it is found that incorrect personal data or information is stored in the information systems, the Corps of Prison and Court Guard shall correct or erasure it without undue delay. If such data was provided, the Corps of Prison and Court Guard shall notify all their recipients.

(3) If the data are stored in the information system of the Corps of Prison and Court Guard no longer needed for completion of tasks, or based upon other legal reason, the Corps of Prison and Court Guard shall erasure the data.

(4) If erasure of personal data could endanger the rights or law protected interests of a data subject, such data shall be restricted.[17i]) Such restricted data shall be possible to be processed only for the purpose that prevented them from being erased.

(5) The Corps of Prison and Court Guard shall verify once in three years if the need for the stored personal data processed still exists.”

The wording of the footnote to reference 17i reads as follows:

“[17i]) point f) of section of Act No. 18/2018 on personal data protection and amending and supplementing certain Acts”.

2. In Section 65d, paragraphs 4 and 5 are deleted.

Current paragraphs 6 and 7 are marked as paragraphs 4 and 5.

Footnote to the reference 18b is deleted.

3. In Section 65d paragraph 5 the words “of paragraph 6” are replaced by the words “of paragraph 4”.

Article VI

Act No. 153/2001 on Prosecution in the wording of Act No. 458/2003, of Act No. 36/2005, of Act No. 59/2009, of finding of the Constitutional Court of the Slovak Republic No. 290/2009, of Act No. 291/2009, of Act No. 102/2010, of Act No. 403/2010, of Act No. 192/2011, of Act No. 220/2011, of Act No. 436/2013, of finding of the Constitutional Court of the Slovak Republic No. 217/2014, of Act No. 401/2015 and of Act No. 125/2016 is amended as follows:

1. The present text of Section 55aa is marked as paragraph 1 and is supplemented by paragraphs 2 and 3 as follows:

“(2) The General Prosecutor's Office in cooperation with other prosecution offices shall verify at least once in 12 months if the processed personal data are still needed for completing the tasks of the prosecution. If the General Prosecutor's Office finds, during verification or during personal data processing, that the data are not needed for performance the tasks of the Prosecutor's Office, it shall erase or anonymise such data without any undue delay.

(3) If the erasure or anonymisation of personal data pursuant to paragraph 2 could endanger the rights or law protected interests of a data subject, the personal data processing may be restricted,[35a]) and they may be processed only for the purpose that has prevented their

erasure.”

In the footnote to reference 35 the words “Act No. 428/2002 as amended” are replaced by the words “Act No. 18/2018 on personal data protection and amending and supplementing certain Acts.”

The footnote to reference 35a reads as follows:

“[35a]) Regulation of the European Parliament and of the Council 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation) (OJ EU L 119, 4. 5. 2016),

Act No. 18/2018 on personal data protection and amending and supplementing certain acts.”

2. In section 55ac, paragraphs 2 and 3 are deleted.

Further, the identification of paragraph 1 is deleted.

Footnote to reference 36 reads as follows:

“[36]) Act No. 18/2018 on personal data protection and amending and supplementing certain acts.”

3. In section 55ad, paragraph 1 is deleted.

Present paragraphs 2 to 4 are marked as paragraphs 1 to 3.

4. In section 55ad paragraph 2 the words “of paragraph 2” are replaced by the words “of paragraph 1”.

5. In point f) paragraph 1 of section 55ae reference 36b and footnote to reference 36b are deleted.

6. Section 55af is deleted, including the footnote to reference 36c.

Article VII

Act No. 483/2001 on Banks as amended in the wording of Act No. 430/2002, Act No. 510/2002, Act No. 165/2003, Act No. 603/2003, Act No. 215/2004, Act No. 554/2004, Act No. 747/2004, Act No. 69/2005, Act No. 340/2005, Act No. 341/2005, Act No. 214/2006, Act No. 644/2006, Act No. 209/2007, Act No. 209/2007, Act No. 659/2007, Act No. 659/2007, Act No. 297/2008, Act No. 552/2008, Act No. 552/2008, Act No. 66/2009, Act No. 186/2009, Act No. 186/2009, Act No. 276/2009, Act No. 492/2009, Act No. 492/2009, Act No. 129/2010, Act No. 129/2010, Act No. 46/2011, Act No. 130/2011, Act No. 314/2011, Act No. 394/2011, Act No. 520/2011, Act No. 547/2011, Act No. 234/2012, Act No. 352/2012, Act No. 132/2013, Act No. 352/2013, Act No. 213/2014, Act No. 213/2014, Act No. 213/2014, Act No. 213/2014, Act No. 371/2014, Act No. 374/2014, Act No. 35/2015, Act No. 252/2015, Act No. 359/2015, Act No. 392/2015, Act No. 405/2015, Act No. 437/2015, Act No. 90/2016, Act No. 91/2016, Act No. 125/2016, Act No. 292/2016, Act No. 298/2016, Act No. 299/2016, Act No. 315/2016, Act No. 386/2016, Act No. 2/2017, Act No. 264/2017 and Act No. 279/2017 is amended as follows:

1. In Section 92a, paragraph 5 reads as follows:

"(5) A client of bank or branches of a foreign banks who is not a natural person shall be entitled to obtain at no charge information from Joint Banking Register regarding himself or herself or its transactions; is entitled at least once a year to request the controller of a Joint Banking Register to receive a name list of persons to whom data were provided on itself or its transactions free of charge; and is entitled to request correction or erasure of incorrect, incomplete or outdated information kept in a Joint Banking register on itself or its transactions free of charge. The client of a bank or branches of foreign bank who is a natural person shall be entitled to access personal data pursuant to a special regulation.[37])."

The footnote to reference 37 reads as follows:

"37) Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation). (OJ EU L 119, 4. 5. 2016).

Act No. 18/2018 on personal data protection and amending and supplementing certain Acts."

2. In Section 92b paragraph 1 and Section 93a paragraphs 2 to 4, the words "and informing" are deleted.

3. In first point a) of section 93a paragraph 1 the after words "and a photography from an identification document" are added after the words "type and number of identification document".

Article VIII

Act No. 395/2002 on Archives and Registries as amended in the wording of Act No. 515/2003, of Act No. 216/2007, of Act No. 335/2007, of Act No. 445/2008, of Act No. 41/2011, of Act No. 305/2013, of Act No. 266/2015 and of Act No. 125/2016 is amended as follows:

1. Footnote to reference 25 reads as follows:

"[25]) Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation). (OJ EU L 119, 4. 5. 2016).

Act No. 18/2018 on personal data protection and amending and supplementing certain Acts."

2. In point a) of section 13 paragraph 5 the word "or" is deleted.

3. In point b) of section 13 paragraph 5 the word "or" is added at the end.

4. In section 13 paragraph 5 is supplemented by point c) that reads as follows:

"c) if the purpose of using the archive document is historical or other scientific research."

Article IX

Act No. 417/2002 on Use of Deoxyribonucleic Acid Analysis for Identification of Persons is amended as follows:

1. Point b) of section 2 reads as follows:

“b) by deoxyribonucleic acid analysis the process of a sample analysis with methods of molecular biology and genetics performed on non-coding segments of a DNA molecule that do not contain information on specific hereditary features; DNA analysis is also understood as prediction of visible phenotypic expressions,”.

2. In point f) is added to section 2, reads as follows:

“f) by prediction of visible phenotypic expressions the analysis of a sample through methods of molecular biology and genetics performed on coding segments of a DNA molecule that contain information, e.g. on colour of hair, colour of eyes and pigmentation of skin.”.

3. The footnote to reference 1 reads:

“[1]) Section 155 paragraphs 2, 3 and 5 and section 156 paragraphs 1 and 2 of Criminal Code of Procedure.

Section 20a of Act of the Slovak National Council No. 171/1993 on Police Force as amended.”.

4. In point a) of section 3 paragraph 1, the words “proceedings, of the Police Force[2]) and Railway Police,[3])” are replaced by words “proceedings and the Police Force[2])”.

The footnote to reference 3 is deleted.

5. Section 3 paragraph 3 reads as follows:

“(3) The sample is taken by a member of the Police Force[2]) (hereafter as “police officer”), law enforcement authority and Prosecutor's Office,[4]) or a court; the sample may be also taken by the person himself or herself in the presence of a police officer, law enforcement authority, Prosecutor's Office or court. Sample-taking pursuant to point b) of paragraph 1 may also be performed based on the written request of a police officer, Prosecutor's Office or court by an officer of the Corps of Prison and Court Guard,[5]) and the subject may take it himself or herself in the presence of an officer of the Corps of Prison and Court Guard. If the sample, which taking to endangers for a physical integrity of human or is to be taken from an intimate part of the human body, it is taken based on the written request of a police officer, Prosecutor's Office or a court by a health care professional with the current necessary expertise.[5a]) The sample must be taken in a way that cannot endanger for the health of the subject or negatively affect for his or her dignity.”.

Footnotes to references 4 and 5 read as follows:

“[4]) Section 10 paragraph 1 of Act No. 301/2005 as amended.

[5]) Act No. 4/2001 on Corps of Prison and Court Guard as amended.

[5a]) Section 33 of Act No. 578/2004 on Health Care Providers, Health Professionals, Professional Organisations in Health Care as amending and supplementing certain Acts.”.

6. In Section 4, a new paragraph 2 is inserted behind paragraph 1 that reads as follows:

“(2) Prediction of visible phenotypic expressions can be only performed from a sample taken in connection with an obviously serious crime,[5b]) crime against life and health, crime against freedom and human dignity,[5c]) or identification of a corpse or separated parts of human body, if DNA analysis does not identify a person in a database or national profiling database of DNA of EU member states pursuant to special regulation.[5d])”.

The present paragraphs 2 to 7 are marked as paragraphs 3 to 8.

Footnotes to references 5b to 5d read as follows:

"[5b]) Section 11 paragraph 3 of the Criminal Code.

[5c]) Section144 to Section 203 of the Criminal Code.

[5d]) Council decision 2008/615/SVV of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ EU L 210/1, 6. 8. 2008).".

7. In Section 4 paragraph 3 the word "of eight" is replaced by word "of twelve".

8. In Section 4 paragraph 4 the following words are added to the end of the introductory sentence: "by accredited methods".

9. In point a) of section 4 paragraph 4 the words "on the list of institutes and other authorities specialised in forensic activities [6])" are replaced with the words "as an expert institution as listed pursuant to a special regulation [6])".

The footnote to reference 6 reads as follows:

"[6]) Act No. 382/2004 on Experts, Interpreters and Translators as amended.".

10. In second sentence of section 4 paragraph 5, the words "for Railway police" are replaced by the words "the court".

11. In Section 4 paragraph 7 the words "in paragraph 5" are replaced by the words "in paragraph 6".

12. In Section 4 paragraph 8 the words "in paragraph 3"are replaced by the words "in paragraph 4".

13. In second point b) of section 5 paragraph 3 the words "and place" are deleted.

14. Footnote to reference 7 reads as follows:

"[7]) Act of the National Council of Slovak Republic No. 171/1993 in the wording of later regulations. Act No. 18/2018 on personal data protection and amending and supplementing certain Acts".

15. In section 8 paragraph 1 reads as follows:

"(1) An authorised unit shall erase the following data from the database

a) on natural person

1. the criminal investigation against whom was terminated since the act for which the criminal proceedings were initiated did not occur or this act is not a crime and there is no justification to put a case or the act was not committed by the person accused of it,[8])

2. who was acquitted since it was not proven that the act for which he or she was under criminal investigation was occurred or since that act is not constituted as a

crime,[9])

b) on a convicted person, person against whom criminal investigation is not admissible10) person against whom criminal investigation has been suspended since the accused person was the legal irresponsibility at the time when the crime was committed due to his mental condition,[11]) and person that was acquitted since he or she is legal irresponsibility due to his or her mental capacity, [12]) after one hundred years have lapsed from his or her birth.".

Footnotes to references 8 to 12 read as follows:

"[8]) Points a) to c) section 215 of paragraph 1 Code of Criminal Procedure.

[9]) Points a) and b) of section 285 Code of Criminal Procedure.

[10]) Section 9 paragraph 1 Code of Criminal Procedure.

[11]) Points e) and f) section 215 paragraph 1 of the Code of Criminal Procedure.

[12]) Points d) and e) section 285 of the Code of Criminal Procedure.".

16. In Section 8 paragraph 3 reads as follows:

"(3) A law enforcement authority, Prosecution Office or court that has completed criminal proceedings against a person whose DNA profile is stored in a database must within three workdays from the termination of criminal proceedings inform the authorised unit.".

17. Annex no. 1 including the title reads as follows:

POLYMORPHOUS SYSTEMS

"Annex no. 1 to Act No. 417/2002

Polymorphous systems of DNA in which the following DNA analysis is performed:

D3S1358

VWA

D8S1179

D21S11

D18S51

HUMTH01

FGA

D1S1656

D2S441

D10S1248

D12S391

D22S1045".

18. Annex no. 2 including the title reads as follows:

“Annex no. 2 to Act No. 417/2002

RESULTS OF DNA ANALYSIS

Institute performing analysis (name and address):

.....

Reasons of analysis:

.....

Biological sample:*

- taken pursuant to point d) section 2 of Act No. 417/2002,
- taken pursuant to section 3 of Act No. 417/2002, while the subject at stake is a subject listed under point a) of section 3 paragraph 1/ point b) of section 3 paragraph 1 / point c) of section 3 paragraph 1 of Act No. 417/2002.

*Strike out any inappropriate option.

DNA Profile**

	Allele 1	Allele 2	Allele 3	Allele 4
D3S1358				
VWA				
D8S1179				
D21S11				
D18S51				
HUMTH01				

FGA				
D1S1656				
D2S441				
D10S1248				
D12S391				
D22S1045				

Personal data on the natural person whose biological sample was secured or taken:

1. name and surname .....

2. date of birth .....

3. birth identification number; for foreigners – number of passport .....

4. address of residence .....

5. citizenship .....

6. other data .....

Information on biological sample secured pursuant to point d) section 2 of Act No. 417/2002

.....

Further information to be provided by.....

(academic degree, name, surname, phone number)

Date:

Name and surname of
responsible employee
signature

Imprint of expert
stamp ”.

Article X

Act No. 586/2003 on the Legal Profession as amended by Act No. 455/1991 licensed trade as amended by Act No. 8/2005, of Act No. 327/2005, of Act No. 331/2007, of Act No. 297/2008, of Act No. 451/2008, of Act No. 304/2009, of Act 136/2010, of Act No. 332/2011, of Act No. 335/2012, of Act No. 339/2013, of Act No. 440/2015, of Act No. 125/2016 is amended as follows:

1. In Section 18, paragraphs 6 and 7 read as follows:

"(6) An lawyer processes personal data of clients and other natural persons in the scope necessary for the purposes of performing his or her profession pursuant to this Act and special regulations.[12b]) A lawyer has, pursuant to the first sentence of this paragraph and pursuant to special regulations, the position of a controller when processing personal data.[12c])

(7) A lawyer is authorised to collect and process personal data necessary for performing advocacy through copying, scanning or otherwise recording official documentation on information storage media without consent of the data subject.".

Footnotes to reference 12b and 12c read as follows:

"[12b]) Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation). (OJ EU L 119, 4. 5. 2016).

[12c]) Article 4 paragraph 7 of the Regulation (EU) 2016/679.".

2. Section 18 is supplemented by paragraphs 8 and 9 that read as follows:

"(8) A lawyer is not obliged to provide information on personal data processing, provide access or portability of personal data pursuant to special regulations,[12d]) if such action could lead to violation of the lawyer's obligation to maintain confidentiality pursuant to this Act.

(9) The Bar Association can adapt by its decision further rights and obligations of the Association, lawyers and data subjects by adopting a Code of Conduct pursuant to a special regulation [12e])".

Footnotes to references 12d and 12e read as follows:

"[12d]) Point d) of article 14 paragraph 5, Article 15 paragraph 4 and Article 20 paragraph 4 of the Regulation (EU) 2016/679.

[12e]) Article 23, Article 40 and Article 90 of the Regulation (EU) 2016/679.".

Article XI

Act No. 541/2004 on Peaceful Use of Nuclear Energy (Atomic Act) as amended in the wording of Act No. 238/2006, of Act No. 21/2007, of Act No. 94/2007, of Act No. 335/2007, of Act No. 408/2008, of Act No. 120/2010, of Act No. 145/2010, of Act No. 350/2011, of Act No. 143/2013, of Act No. 314/2014, of act No. 54/2015, of Act No. 91/2016, of Act No. 125/2016 and of Act No. 96/2017 is amended as follows:

1. In Section 26, paragraph 6 reads as follows:

"(6) A authorisation holder shall ensure that for permitting and control of entries of persons into the nuclear facility shall identify persons through their identification documents or other identification document such as a passport or UN travel document that contains the person's academic degree, name and surname, date of birth, permanent address, number of identification document or number of other identification document, citizenship, biometric data, birth identification number and photograph and further, in nuclear facilities where there is nuclear material classified as category I or II pursuant to a special regulation,[37a]) the authorisation holder shall ensure that for permitting and control of entries of persons into guarded area and internal area shall also identify persons using biometric data.[37b]) Persons entering or leaving a nuclear facility shall tolerate identification pursuant to the first sentence. If these persons refuse to tolerate identification pursuant to the first sentence, the authorisation holder shall prevent them from entering or leaving the nuclear facility. The authorisation holder is authorised to process personal data pursuant to the first sentence according to a special regulation [37c])".

Footnotes to references 37b and 37c read as follows:

"[37b]) Point g) of article 9 paragraph 2 Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation) (OJ EU L 119, 4. 5. 2016).

[37c]) Point c) article 6 paragraph 1 of Regulation (EU) 2016/679.

Act No. 18/2018 on personal data protection and amending and supplementing certain Acts".

2. Section 31 is supplemented by paragraph 17 that reads as follows:

"(17) The Authority is, pursuant to a special regulation[41a]), authorised to process the personal data of inspectors, trainee inspectors, international inspectors and other natural persons called to the inspection or international inspection when performing their inspection duties, as well as of other natural persons, for the purposes of facilitating control of entries and exits of those persons to/from the nuclear facility in the scope of personal data specified under section 26 paragraph 6. The Authority is authorised to provide personal data pursuant to the first sentence to the authorisation holder for the same purpose and in the same scope as specified in the first sentence.".

Footnote to reference 41a reads as follows:

"[41a]) Point e) of article 6 paragraph 1 of Regulation (EU) 2016/679.

Act No. 18/2018 on personal data protection and amending and supplementing certain Acts".

Article XII

Act No. 652/2004 on Public Administration Authorities in the field of Customs as amended and in the wording of Act No. 331/2005, of Act No. 191/2007, of Act No. 537/2007, of Act No. 166/2008, of Act No. 491/2008 , of Act No. 207/2009, of Act No. 305/2009, of Act No. 465/2009, of Act No. 508/2010, of Act No. 192/2011, of Act No. 256/2011, of Act No. 331/2011, of Act No. 546/2011, of Act No. 441/2012, of Act No. 207/2014, of Act No. 307/2014, of Act No. 333/2014, of Act No. 360/2015, of Act No. 397/2015 and of Act No. 298/2016 is amended as follows:

1. In section 52, paragraph 5 is deleted.

The present paragraphs 6 to 9 are marked as paragraphs 5 to 8.

2. In section 54, paragraph 6 is deleted.

3. In section 54b paragraph 4, the words “in Section 55 par. 4” are replaced by the words “pursuant to a special regulation.[46ba])”.

Footnote to reference 46ba reads as follows:

“[46ba]) Section 64 of Act No. 18/2018 on personal data protection and amending and supplementing certain Acts.”.

4. In section 54c, paragraphs 3 to 5 are deleted.

5. In section 55, the title under the section and paragraphs 1 and 4 to 11 are deleted, including the footnote to reference 46f.

The present paragraphs 2 and 3 are marked as paragraphs 1 and 2.

6. In section 58, paragraph 8 is deleted.

Article XIII

Act No. 757/2004 on Courts as amended and in the wording of Act No. 517/2008, of Act No. 59/2009, of Constitutional Court finding No. 290/2009, of Act No. 291/2009, of Act No. 318/2009, of Act No. 33/2011, of Act No. 192/2011, of Act No. 467/2011, of Act No. 335/2012, of Act No. 195/2014, of the Slovak Constitutional Court finding No. 216/2014, of Act No. 322/2014, of Act No. 87/2015, of Act No. 125/2016, of Act No. 301/2016, of Act No. 2/2017 and of Act No. 152/2017 is amended as follows:

1. The footnote to reference 34 reads as follows:

“34) Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation) (OJ EU L 119, 4. 5. 2016).

Act No. 18/2018 on personal data protection and amending and supplementing certain Acts.”.

2. In section 79, paragraph 1 reads as follows:

“(1) The ministry and courts process information, personal data and other types of data (hereafter as “data”) regarding civil court proceedings and criminal proceedings in the public interest, as well as data collected while fulfilling their tasks resulting from special regulations,38) including personal data regarding representation of the Slovak Republic at the Court of Justice of the European Union and in phases prior to those proceedings as well as related to personnel issues relevant for the Court of Justice of the European Union.”.

3. The present wording of section 80 is marked as paragraph 1 and is supplemented by paragraph 2 that reads as follows:

“(2) Personal data related to representation of the Slovak Republic in proceedings at the

Court of Justice of the European Union and in phases prior to these proceedings as well as personnel issues regarding the Court of Justice of the European Union may be provided by the Ministry, including for fulfilment of tasks pursuant to a special regulation39) to other public authorities or other recipients."

4. In section 81, paragraph 1 is deleted and the identification of paragraph 2 is deleted.

5. In section 82d, the reference "[34])" above the word "Act" is replaced by reference "[42c])".

The footnote to reference 42c reads as follows:

"[42c]) Act No. 18/2018 on personal data protection and amending and supplementing certain Acts.".

6. In Section 82e, paragraph 1 is deleted.

Present paragraphs 2 to 5 are marked as paragraphs 1 to 4.

7. In Section 82e paragraph 2, the words "of paragraphs 2" are replaced by the words "of paragraphs 1".

8. In point f) of section 82f paragraph 1, the reference 42d and footnote to reference 42d are deleted.

9. Section 82g, including footnote to reference 42e is deleted.

Article XIV

Act No. 129/2010 on Consumer loans and other loans to consumers as amended in the wording of Act No. 394/2011, Act No. 352/2012, Act No. 132/2013, Act No. 102/2014, Act No. 106/2014, Act No. 373/2014, Act No. 35/2015, Act No. 117/2015, Act No. 389/2015 of Act No. 438/2015, of Act No. 90/2016, of Act No. 91/2016, of Act No. 299/2016 and of Act No. 279/2017 is amended as follows:

1. In section 1 paragraph 6 the words "up to 15" are replaced with "up to 14".

2. In section 7 paragraph 14 is deleted.

Current paragraphs 15 to 43 are marked as paragraphs 14 to 42.

3. In section 7 paragraph 4 the words "17 and 18" are replaced by words "16 and 17".

4. In section 7 paragraph 21, the number "21" after the word "paragraph" is replaced by the number "20".

5. In section 7 paragraph 24, introductory sentence, the words "20 to 24" are replaced by the words "19 to 23".

6. In section 7 paragraph 25 the number "25" is replaced by the number "24" and the number "39" is replaced by the number "38".

7. In section 7 paragraph 26, the number "20" in the introductory sentence is replaced by the number "19".

8. In section 7 paragraph 27 the words “of paragraph 20” are replaced by the words “of paragraph 19“.

9. In section 7 paragraph 29 the number “32” is replaced by the number “31“.

10. In section 7 paragraph 30 the number “30” is replaced by the number “29”.

11. In section 7 paragraph 31 in the introductory sentence the words “30 and 31” are replaced by the words “29 and 30”.

12. In section 7 paragraph 33, introductory sentence, the words “35, 36 and 38” are replaced by the words “34, 35 and 37”, and the number “33” is replaced by the number “32”.

13. In section 7 paragraph 34 to 38 the number “34” is replaced by the number “33”.

14. In section 7 paragraph 38 the number “26” is replaced by the number “25”.

15. In section 7 paragraph 40 the words “20 to 40” are replaced by the words “19 to 39” and the words “17 to 19” are replaced by the words “16 to 18”.

16. In the point a) of section 7 paragraph 41 the words “25 and 32” are replaced by the words “24 and 31”.

17. In section 11 paragraph 2 the words “20 to 43” are replaced by the words “19 to 42”.

18. In the point b) of section 20a paragraph 3, the words “information and demonstration of identity pursuant to a special regulation” are inserted before the word “founding document” “[32b])”.

19. In point h) of section 20a paragraph 3 and point e) of section 20b paragraph 5 the words “16 to 18” are replaced by the words “15 to 17”.

20. In section 24 paragraph 1 the words “17 to 43” are replaced by the words “16 to 42”.

21. In point b) of section 24 paragraph 6 the words “name, surname, permanent address, citizenship and date of birth” are replaced by the words “information and proof of identity pursuant to a special regulation[32b])”.

22. In point h) of section 24 paragraph 7 the words “17 to 19” are replaced by the words “16 to 18”.

Article XV

Act No. 39/2015 on Insurance as amended the wording of Act No. 359/2015, of Act No. 437/2015, of Act No. 125/2016, of Act No. 292/2016, of Act No. 339/2016 and of Act No. 282/2017 is amended as follows:

In section 72, paragraph 13 is deleted.

Present paragraph 14 is marked as paragraph 13.

Article XVI

This Act comes into force on 25 May 2018.

Andrej Kiska [signature]

Andrej Danko [signature]

Robert Fico [signature]

1) Section 57 paragraph 2 of Act No. 351/2011 on Electronic Communications as amended.

2) Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/ES (General Data Protection Regulation) (OJ EU L 119, 4. 5. 2016).

3) Section 17 paragraph 9 of Act of the National Council of Slovak Republic No. 46/1993 on the Slovak Information Service in the wording of Act No. 192/2011

4) Section 17 paragraph 6 of Act of the National Council of Slovak Republic No. 198/1994 on Military Intelligence in the wording of Act No. 444/2015 Section 14 paragraph 7 of Act No. 281/2015 on Civil Service of Professional Soldiers as amended.

5) Act No. 215/2004 on the Protection of Classified Information as amended.

6) Act No. 552/2003 on the Performance of Work in the Public Interest as amended.

7) Act No. 55/2017 on Civil Service as amended.

8) For example, Act of the National Council of Slovak Republic No. 171/1993 on the Police Forces as amended, Act No. 540/2001 on State Statistics as amended, Act No. 395/2002 on Archives and Registries as amended or Act No. 553/2002 on Disclosure of State Security Authorities in the Period of 1939-1989 and on founding the Nation's Memory Institute as amended (Act on Nation's Memory) as amended.

9) Act No. 22/2004 on Electronic Commerce amending and supplementing Act No. 128/2002 on State Control of the Internal Market in the Consumer Protection Matters as amended, in the wording of Act No. 284/2002 as amended.

10) Act No. 36/2005 on Family as amended.

11) For example, the Labour Code as amended, Act No. 461/2003 on Social Insurance as amended or Act No. 5/2004 on Employment services as amended.

12) For example, the Civil Code, Commercial Code, Act No. 250/2007 on Consumer Protection as amending Act of the Slovak National Council No. 372/1990 on Misdemeanours as amended, Act No. 90/2016 on Mortgages as amended.

13) Act No. 447/2008 on Financial Contributions to Compensate Severe Health Disability as amended.

14) Act No. 328/2002 on Social Security for Police Officers and Soldiers as amended.

15) For example, Act No. 576/2004 on Health Care, Services Related to Provision of Health Care as amended.

16) Act No. 330/2007 on Register of Convictions and Disqualifications as amended.

17) Section 2 paragraph 15 of Act No. 395/2002 as amended.

18) Section 20 of Act No. 395/2002 as amended.

19) For example, Civil Adversarial Code, Code of Administrative Court Procedure.

20) Civil Adversarial Code.

21) Act No. 757/2004 on Courts as amended, Code of Criminal Procedure.

22) Act of the National Council of Slovak Republic No. 301/1995 on Birth Identification Number as amended by Act No. 515/2003

23) Section 116 of the Civil Code.

24) Article 15, 16, 18 and 21 of EU regulation (EU) 2016/679.

25) Article 15, 16, 18 through 21 of EU regulation (EU) 2016/679.

26) For example, Act of the National Council of Slovak Republic No. 566/1992 on National bank of Slovakia as amended, Act of the Slovak National Council No. 46/1993 as amended, Act of the Slovak National Council No. 171/1993 as amended, Act No. 215/2004 as amended, Act No. 563/2009 on Tax on motor vehicles as amended, Act No. 307/2014 on Certain measures related to reporting of activities not in society´s interests and on amendment and supplements to certain acts.

27) Section 21 paragraph 1 and point a) of paragraph 5 of Act No. 523/2004 on Budget rules of the public service as amended.

28) Article 51 paragraph 1 of the EU regulation (EU) 2016/679.

29) Article 57 paragraph 1 and Article 58 paragraph 1 to 3 of the EU regulation (EU) 2016/679.

30) For example, article 56, 60 to 62 of the EU regulation (EU) 2016/679.

31) Article 68 of the EU regulation (EU) 2016/679.

32) Article 56, 60 and Article 61 paragraph 1 to 8 of the EU regulation (EU) 2016/679.

33) For example, Act No. 215/2004 as amended.

34) Section 60 of the Act of the National Council of Slovak Republic No. 350/1996 on the Rules of procedure of the National Council of Slovak Republic as amended by Act No. 215/2004.

35) Constitutional Act No. 357/2004 on Protecting public interest in the service of public officials in the wording of Act No. 545/2005.

Section 112 of Act No. 55/2017

36) For example, Penal Code, Administrative court procedure

37) Sections 38 and 40 of Act No. 215/2004 as amended.

38) Article 40 paragraph 2 of the EU regulation (EU) 2016/679.

39) Article 40 paragraph 7 of the EU regulation (EU) 2016/679.

40) Point b) of article 64 paragraph 1 of the EU regulation (EU) 2016/679.

41) Act No. 395/2002 as amended.

42) Act No. 395/2002 as amended.

Article 41 of the EU regulation (EU) 2016/679.

43) Article 43 paragraphs 2 and 3 of the EU regulation (EU) 2016/679.

44) Article 62 of the EU regulation (EU) 2016/679.

45) Act of the National Council of Slovak Republic No. 10/1996 on Control in the state administration as amended.

46) Article 56 paragraph 1 of the EU regulation (EU) 2016/679.

47) Article 56 of the EU regulation (EU) 2016/679.

48) Act No. 71/1967 on Administrative procedures (Administrative Code) as amended.

Annex to Act No. 18/2018

LIST OF TRANSPOSED LEGALLY BINDING ACTS OF THE EUROPEAN UNION

Directive of the European Parliament and the Council (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of the personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ EU L 119, 4. 5. 2016).