

PERSONAL DATA PROTECTION ACT

Passed 12 February 2003

(RT¹ I 2003, 26, 158),

entered into force 1 October 2003.

amended by the following Acts:

14.04.2004 entered into force 01.05.2004 – RT I 2004, 30, 208.

25.01.2007 entered into force 18.02.2007 – RT I 2007, 11, 53

Chapter 1

GENERAL PROVISIONS

§ 1. Purpose of Act

The purpose of this Act is protection of the fundamental rights and freedoms of natural persons in accordance with public interests with regard to processing of personal data.

§ 2. Scope of application of Act

(1) This Act provides for:

- 1) the conditions and procedure for the processing of personal data;
- 2) the procedure for the exercise of state supervision over the processing of personal data;
- 3) the liability for violation of the personal data processing requirements.

(2) The following are excluded from the scope of this Act:

- 1) processing of personal data by natural persons for personal use;
- 2) processing of personal data lawfully designated for public use;
- 3) transmission of personal data through the territory of Estonia without processing the data in Estonia in any other manner;
- 4) (Repealed - 25.01.2007 entered into force 18.02.2007 – RT I 2007, 11, 53)

(3) This act provides for processing of state secrets containing personal data, if such processing is provided for in:

- 1) Convention from 19 July 1990 Applying the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders (the Schengen Convention) or
- 2) Convention from 26 July 1995 based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (the Europol Convention).

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 3. Application of Administrative Procedure Act

The provisions of the Administrative Procedure Act (RT I 2001, 58, 354; 2002, 53, 336; 61, 375) apply to the administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

§ 4. Personal data

(1) Personal data are information relating to an identified natural person or a natural person identifiable by reference to the person's physical, mental, physiological, economic, cultural or social characteristics, relations and associations.

(2) The following are private personal data:

- 1) data revealing details of family life;
- 2) data revealing an application for the provision of social assistance or social services;
- 3) data revealing mental or physical suffering endured by a person;

4) data collected on a person during the process of taxation, except data concerning tax arrears.

(3) The following are sensitive personal data:

1) data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a legal person in private law registered pursuant to the procedure provided by law;

2) data revealing ethnic or racial origin;

3) data relating to the state of health or disability;

4) data relating to genetic information;

5) data relating to sexual life;

6) data concerning membership in trade unions;

7) information collected in criminal proceedings or in other proceedings to ascertain an offence before a public court session or before a judgment is made in a matter concerning an offence, or if this is necessary in order to protect public morality or the family and private life of persons, or where the interests of a minor, a victim, a witness or justice so require.

§ 5. Processing of personal data

Processing of personal data means any operation or set of operations which is performed upon personal data, such as collection, recording, organisation, storage, alteration, grant of access, consultation, retrieval, use, transmission, cross-usage, combination, blocking, erasure or destruction, or several of the aforementioned operations regardless of the manner in which they are performed or the means used.

§ 6. Principles of processing of personal data

In the processing of personal data, chief processors and authorised processors of personal data are required to take guidance from the following principles:

1) the principle of legality – personal data may be collected in an honest and legal manner;

2) the principle of purposefulness – personal data may be collected only for specified and legitimate purposes and personal data shall not be processed in a manner which fails to comply with the purposes of data processing;

3) the principle of minimality – personal data may be collected only to the extent which is necessary for the purposes for which they are collected;

4) the principle of restriction on use – personal data may be used for other purposes only with the consent of the data subject or with the permission of a competent body;

5) the principle of data quality – personal data shall be kept up to date, be complete and necessary for the given purpose of data processing;

6) the principle of security – security measures to prevent the involuntary or unauthorised alteration, disclosure or destruction of personal data shall be applied in order to protect the data;

7) the principle of individual participation – a data subject shall be notified of data collected thereon, access to data pertaining to the data subject shall be ensured to him or her and the data subject has the right to demand the rectification of inaccurate or misleading data.

§ 7. Chief processor

(1) A chief processor is a natural or legal person, or a state or local government agency who processes personal data or at whose request personal data are processed. A chief processor may be determined by an Act or Regulation.

(2) Unless otherwise provided by an Act or Regulation, a chief processor shall determine:

1) the purposes of processing of personal data;

2) the categories of personal data to be processed;

- 3) the procedure for and manner of processing personal data;
- 4) permission for transmission of personal data to third persons.

§ 8. Authorised processor

An authorised processor is a natural or legal person, or a state or local government agency who processes personal data at the request of a chief processor pursuant to administrative legislation or contracts. Administrative legislation or contracts shall determine the procedure for, manner of and conditions for processing personal data. An authorised processor may be determined by an Act or Regulation.

§ 9. Data subject

A data subject is a person whose personal data are processed.

§ 10. Third person

(1) A third person is a natural or legal person, or a state or local government agency who is not:

- 1) a chief processor;
- 2) an authorised processor;
- 3) a data subject;
- 4) a person who is subordinate to a chief processor or authorised processor and who processes personal data.

(2) A third person who processes personal data disclosed to the third person by a chief processor is deemed to be a chief processor within the meaning of subsection 7 (1) of this Act, and the third person is required to comply with the requirements of this Act, other Acts and legislation established on the basis thereof in processing personal data.

Chapter 2

PERMISSION FOR PROCESSING PERSONAL DATA

§ 11. Permission for processing personal data

(1) Personal data may be processed only with the permission of the data subject, unless otherwise provided by law.

(2) An administrative authority may process personal data only in the course of performance of public duties in order to perform an obligation prescribed by law or international agreements.

(3) the conditions and procedure of processing personal data provided for in clause 2 (3) shall be provided for by the Government of the Republic.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 12. Processing of personal data with consent of data subject

(1) Consent for the processing of personal data means a freely given specific and informed indication of the wishes of a data subject by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

(2) Before obtaining the consent of a data subject for the processing of personal data, the chief processor or authorised processor shall notify the data subject of the following:

- 1) the purpose of processing of the personal data;
- 2) persons or categories thereof to whom transmission of the personal data is permitted;
- 3) the name of the chief processor or a representative thereof and the address of the place of business of the chief processor;

4) the cases when the data subject has the right to demand termination of processing of the personal data and rectification, blocking or erasure of the personal data;

5) the cases when the data subject has the right to obtain access to the personal data pertaining to him or her.

(3) The consent of a data subject shall be valid during the life of the data subject and thirty years after the death of the data subject, unless the data subject has decided otherwise.

(4) A data subject may withdraw his or her consent at any time. Withdrawal of consent has no retroactive effect. The provisions concerning declarations of intention in the General Part of the Civil Code Act (RT I 2002, 35, 216; 2003, 13, 64) shall additionally apply to the consent.

(5) In the case of a dispute, a data subject is presumed not to have granted consent for the processing of personal data relating to him or her.

(6) This section does not apply if personal data are processed by an administrative authority, except upon processing of sensitive personal data specified in subsection 4 (3) of this Act.

§ 13. Processing of personal data after death of data subject

(1) After the death of a data subject, processing of personal data relating to the data subject is permitted only with the written consent of the spouse, a parent, grandparent, child, grandchild, brother or sister of the data subject, except if consent is not required for processing of the personal data or if thirty years have passed from the death of the data subject.

(2) Subsection (1) of this section does not apply if only the name, gender, date of birth and death and the fact of death are the personal data to be processed.

§ 14. Processing of personal data without consent of data subject

(1) Processing of personal data without the consent of a data subject is permitted if the personal data are processed:

1) for performance of a contract entered into with the data subject or ensuring performance of the contract;

2) for protection of the life, health or freedom of the data subject or other person;

3) for performance of an obligation prescribed by law or international agreements.

(2) Transmission of personal data or grant of access to the data to third persons without the consent of a data subject is permitted:

1) if the person to whom the data are transmitted processes personal data for performance of obligations prescribed by law;

2) for protection of the life, health or freedom of the data subject or other person;

3) if the third person requests information which is obtained or created upon performance of public duties provided by law or legislation issued on the basis thereof and access to the information is not restricted.

(3) Processing of sensitive personal data and private personal data without the consent of a data subject is permitted:

1) for performance of an obligation prescribed by law or international agreements;

2) for protection of the life, health or freedom of the data subject or other person.

(4) Transmission of sensitive personal data and private personal data or grant of access to the data to third persons without the consent of a data subject is permitted:

1) if the person to whom the data are transmitted processes sensitive personal data or private personal data for performance of an obligation prescribed by law or international agreements;

2) for protection of the life, health or freedom of the data subject or other person.

(5) Data relating to the state of health of a data subject who is in hospital may be transmitted or the data may be accessed by those closest to him or her, except if:

- 1) the data subject has prohibited access to the data or transmission of the data;
- 2) a body conducting an investigation has prohibited access to the data or transmission of the data in the interests of preventing a criminal offence, of apprehending a criminal offender or ascertaining the truth in a criminal proceeding.

§ 15. Notification of data subject of processing of personal data

(1) If a data subject is not the source of personal data, the chief processor or authorised processor shall notify a third person before the transmission of personal data or the data subject after obtaining the personal data of:

- 1) the purpose of processing of the personal data;
- 2) the categories and sources of the personal data;
- 3) persons or categories thereof to whom transmission of the personal data is permitted;
- 4) the name of the chief processor or a representative thereof and the address of the place of business of the chief processor;
- 5) the cases when the data subject has the right to demand termination of processing of the personal data and rectification, blocking or erasure of the personal data;
- 6) the cases when the data subject has the right to obtain access to the personal data pertaining to him or her.

(2) The obligation specified in subsection (1) of this section does not apply:

- 1) if the data subject is aware of the circumstances listed in subsection (1);
- 2) if personal data are processed for performance of an obligation prescribed by law or international agreements;
- 3) in the cases provided for in subsection 30 (1) of this Act.

§ 16. Permission for processing personal identification code

Processing of a personal identification code is permitted without the consent of the data subject if processing of the personal identification code is prescribed in an international agreement, an Act or Regulation.

§ 17. Automated decisions

(1) Making of a decision by a data processing system without the participation of a natural person (hereinafter automated decision) is prohibited if the character, abilities or other characteristics of a data subject are assessed by the decision or it brings about legal consequences for the data subject or significantly affects the data subject in any other manner, except in the following cases:

- 1) an automated decision in respect of the data subject is made in the course of entry into or performance of a contract provided that the application of the data subject for entry into or performance of the contract is satisfied or the data subject is granted an opportunity to file an objection against the decision being made for the protection of his or her legitimate interest;
- 2) making of an automated decision is prescribed by law if measures for the protection of the legitimate interests of the data subject are provided by law.

(2) Before making of an automated decision, a data subject shall, in an unambiguous manner, give notification of the process and conditions of data processing which are the basis for making of the automated decision.

Chapter 3

PERSONAL DATA PROCESSING REQUIREMENTS AND SECURITY MEASURES TO PROTECT PERSONAL DATA

§ 18. Personal data processing requirements

In the processing of personal data, chief processors and authorised processors are required to:

- 1) promptly erase or block personal data unnecessary for the given purposes unless otherwise prescribed by law;
- 2) ensure that personal data are correct and, if necessary for the given purposes, up to date;
- 3) block incomplete and inaccurate personal data and immediately take the necessary measures for the amendment or rectification of the data;
- 4) store inaccurate data with a notation concerning their period of use together with accurate data;
- 5) block personal data which are contested on the basis of accuracy until the accuracy of the data is verified or the accurate data are determined.

§ 19. Organisational, physical and IT security measures to protect personal data

(1) In order to protect personal data, chief processors and authorised processors are required to take organisational, physical and IT security measures:

- 1) as regards the integrity of the data, against accidental or intentional unauthorised alteration of data;
- 2) as regards the availability of the data, against accidental loss and intentional destruction and against prevention of access to the data for entitled persons;
- 3) as regards the confidentiality of the data, against unauthorised processing.

(2) In the processing of personal data, chief processors and authorised processors are required to:

- 1) prevent the access of unauthorised persons to equipment used for processing personal data;
- 2) avoid unauthorised reading, copying and alteration in the data processing system and unauthorised removal of data media;
- 3) prevent the unauthorised recording, alteration or erasure of personal data and ensure that it be subsequently possible to determine when, by whom and which personal data were recorded, altered or erased;
- 4) ensure that every user of a data processing system only has access to personal data permitted to be processed by him or her and to the data processing permitted for him or her;
- 5) ensure the existence of information on the transmission of personal data regarding when, to whom and which personal data were transmitted and the unaltered storage of such data;
- 6) ensure that unauthorised reading, copying, alteration or erasure of personal data is not carried out in the transmission of the personal data by data communication equipment and in the transportation of data media;
- 7) organise the work of enterprises, agencies and associations in a manner that allows compliance with data protection requirements.

(3) Chief processors and authorised processors are required to maintain records on the devices and software which are under the supervision thereof and used in the processing of personal data and they shall document the following information:

- 1) the name, type and location of the device and the name of the manufacturer of the device;
- 2) the name and version and the name and details of the manufacturer of the software and the location of the documents of the software.

§ 20. Requirements for persons who process personal data

(1) Persons who are subordinate to chief processors or authorised processors and who process personal data are required to process such for the purposes and under the conditions specified in this Act and according to the orders and instructions provided by the chief processors.

(2) The persons specified in subsection (1) of this section are required to maintain the confidentiality of personal data which become known to them in the performance of their duties even after performance of their duties relating to the processing, or after termination of their employment or service relationships.

(3) Chief processors and authorised processors are required to ensure the training in personal data protection to persons subordinate to them who process personal data.

Chapter 4

NOTIFICATION OF PROCESSING OF PERSONAL DATA

§ 21. Notification obligation

(1) A chief processor of personal data is required to notify the Data Protection Inspectorate of processing of private personal data if the private personal data are processed in digital form with a computer or in a file of papers where the private personal data are easily accessible on the basis of certain criteria.

(2) The notification obligation does not apply if personal data are processed in a general national register or a state register or if the personal data are processed pursuant to an Act or Regulation.

§ 22. Notice concerning processing of personal data

(1) In order to perform a notification obligation specified in subsection 21 (1) of this Act, a chief processor of personal data shall submit a notice concerning processing of private personal data (hereinafter notice).

(2) A notice concerning processing of personal data shall be submitted as a digital entry in the register of processors of personal data at least one month before processing of the personal data commences.

(3) A notice shall set out:

1) the name, registry code or personal identification code, place of business, seat or residence and details (postal address, telephone number, e-mail address etc) of the chief processor and authorised processor;

2) the purposes of processing of the personal data;

3) the categories of the personal data;

4) the categories of persons whose data are processed;

5) the sources of the personal data;

6) persons or categories thereof to whom transmission of the personal data is permitted;

7) the conditions for transmission of the personal data to foreign states;

8) the conditions for the blocking, erasure and destruction of the personal data;

9) a general description of organisational, physical and IT security measures to protect personal data specified in subsection 19 (2) of this Act.

(4) A notification obligation is deemed to be performed as of entry of the notice in the register of processors of personal data.

§ 23. Notification of alteration of data

A chief processor is required to notify the Data Protection Inspectorate of the alteration or amendment of the data entered in the register of processors of personal data before implementation of the corresponding alterations or amendments pursuant to the procedure provided for in § 22 of this Act.

Chapter 5

REGISTRATION OF PROCESSING SENSITIVE PERSONAL DATA

§ 24. Obligation to register processing of sensitive personal data

(1) Chief processors are required to register processing of sensitive personal data with the Data Protection Inspectorate.

(2) A chief processor who applies for an activity licence or a licence in an area of activity which involves processing of sensitive personal data is, before application for the activity licence or licence, required to register the processing with the Data Protection Inspectorate. The activity licence or licence shall not be issued unless the processing of personal data is registered.

(3) Processing of sensitive personal data shall be registered for a term of five years. At least three months before expiry of the term, a chief processor is required to submit a new registration application which complies with the requirements of § 25 of this Act. Upon expiry of the term, the chief processor loses the right to process sensitive personal data.

(4) Processing of sensitive personal data is prohibited:

1) upon failure to register the processing of sensitive personal data with the Data Protection Inspectorate;

2) if the term for the registration of processing of sensitive personal data has expired and the chief processor has not submitted a new registration application;

3) if the Data Protection Inspectorate has suspended or prohibited the processing of sensitive personal data.

(5) The Data Protection Inspectorate shall refuse to register processing of sensitive personal data if:

1) there is no legal basis for the processing;

2) the conditions for processing do not comply with the requirements of this Act, another Act or legislation issued on the basis thereof;

3) the applied organisational, physical and IT security measures to protect personal data do not ensure compliance with the requirements provided for in § 19 of this Act.

§ 25. Registration application

(1) A registration application shall be submitted to the Data Protection Inspectorate in digital form through its web site for entry in the register of processors of personal data at least one month before processing of sensitive personal data commences.

(2) A registration application shall set out the following:

1) the name, registry code or personal identification code, place of business, seat or residence and details (postal address, telephone number, e-mail address etc) of the chief processor and authorised processor;

2) the purposes of processing of the personal data;

3) the categories of the personal data;

4) the categories of persons whose data are processed;

5) the sources of the personal data;

6) persons or categories thereof to whom transmission of the personal data is permitted;

- 7) the conditions for transmission of the personal data to foreign states;
- 8) a detailed description of organisational, physical and IT security measures to protect personal data specified in subsection 19 (2) of this Act.

§ 26. Processing of registration application

- (1) The Data Protection Inspectorate shall decide to register or refuse to register the processing within twenty working days as of the date of submission of the registration application.
- (2) The Data Protection Inspectorate may inspect the preparedness for the processing of personal data on site. In such case, the term for the adjudication of the registration application is extended by ten working days. As a result of inspection, the Data Protection Inspectorate may give recommendations for the application and strengthening of organisational, physical and IT security measures to protect personal data.
- (3) The right of a chief processor to process sensitive personal data arises as of the date determined in the decision specified in subsection (1) of this section. If the decision specified in subsection (1) of this section does not specify a term, the chief processor has the right to process sensitive personal data as of the date following the date of entry of the decision in the register of processors of personal data.
- (4) A decision to register processing of sensitive personal data is deemed to have been delivered to the chief processor upon disclosure of the decision on the web site of the Data Protection Inspectorate. A notation concerning a decision to refuse to register shall be made in the register of processors of personal data and the applicant shall be notified of the decision by delivery thereof.
- (5) A chief processor is required to register the alteration or amendment of data entered in the register of processors of personal data with the Data Protection Inspectorate. The provisions concerning the terms for the registration of processing of personal data apply to the registration of alteration or amendment of data.

§ 27. Register of processors of personal data

- (1) The register of processors of personal data is a database maintained by the Data Protection Inspectorate pursuant to the procedure established by the Government of the Republic in which notices concerning the processing of private personal data and information concerning registration of processing of sensitive personal data are registered.
- (2) Information submitted to the Data Protection Inspectorate concerning the organisational, physical and IT security measures to protect personal data, and information concerning the conditions of blocking, erasure or destruction of personal data is deemed to be information intended for internal use.
- (3) A register means information which is on the web site of the Data Protection Inspectorate for public use, except information specified in subsection (2) of this section and information pertaining to the processing of personal data in security authorities.
- (4) Data entered in the register are informative. Entries concerning the registration of processing of sensitive personal data have legal effect.

Chapter 6

TRANSMISSION OF PERSONAL DATA TO FOREIGN STATES

§ 28. Transmission of personal data to foreign states

- (1) Personal data from a database located in Estonia may be transmitted to a state with a sufficient level of data protection.

- (2) (Repealed - 14.04.2004 entered into force 01.05.2004 - RT I 2004, 30, 208)
- (3) Transmission of personal data is permitted to the Member States of the European Union, state parties to the Agreement of the European Economic Area and to states the data protection level of which is deemed to be sufficient by the Commission of the European Communities. Transmission of personal data is not permitted to states the data protection level of which is deemed to be insufficient by the Commission of the European Communities.
- (4) Personal data may be transmitted to a foreign state which does not meet the condition provided for in subsection (1) of this section only with the permission of the Data Protection Inspectorate:
- 1) if, in the specific case, the chief processor guarantees the protection of the rights and private life of the data subject in the state;
 - 2) in the specific case of transmission of personal data, the sufficient level of data protection is ensured in the state. Upon assessment of the level of data protection, circumstances related to the transmission of personal data, including the categories of data, the purposes and duration of processing, transmission of data to the country of destination and to the final country of destination and the law of the state shall be taken into account.
- (5) The Data Protection Inspectorate shall inform the Commission of the European Communities of a permission granted pursuant to subsection (4) of this section.
- (6) Without the permission of the Data Protection Inspectorate, personal data may be transmitted to a foreign state where the sufficient level of data protection is not ensured:
- 1) if the data subject has consented thereto;
 - 2) in the cases provided for in subsection 14 (2) of this Act;
 - 3) if the data are transmitted to the foreign state in cryptographic form and the data necessary for decoding is not communicated to the foreign state.
- (RT I 2004, 30, 208 – entered into force 01.05.2004)

Chapter 7 RIGHTS OF DATA SUBJECT

§ 29. Right of data subject to receive information and personal data relating to him or her in processing of personal data

- (1) At the request of a data subject, the chief processor and the authorised processor shall notify the data subject of the following:
- 1) the personal data relating to him or her;
 - 2) the purposes of processing of the personal data;
 - 3) the categories and sources of the personal data;
 - 4) third persons or categories thereof to whom transmission of the personal data is permitted;
 - 5) the name and address of the place of business of the chief processor.
- (2) A data subject has the right to receive copies of personal data relating to him or her from a chief processor or authorised processor. The chief processor or authorised processor may charge up to 3 kroons per page for copies on paper starting from the twenty-first page. A fee for the release of personal data may be charged also for the repeated release of the same personal data.
- (3) A chief processor or authorised processor is required to provide a data subject with information and the requested personal data or state the reasons for refusal to provide data or information within five working days after the date of receipt of an application.

§ 30. Exceptions to right to receive information and personal data

(1) The right of a data subject to receive information and personal data relating to him or her in the processing of personal data is restricted if this may prejudice:

- 1) the rights and freedoms of other persons;
- 2) protection of the confidentiality of filiation of a child;
- 3) prevention of a criminal offence or apprehension of a criminal offender;
- 4) ascertainment of the truth in a criminal proceeding.

(2) A chief processor shall make a decision to refuse to provide data or information and shall notify the data subject thereof.

§ 31. Right of data subject to demand termination of processing of personal data and rectification, blocking and erasure of personal data

(1) If processing is contrary to this Act, other Acts or legislation established on the basis thereof, a chief processor or authorised processor is, at the request of the data subject, required to:

- 1) terminate the processing of personal data relating to him or her;
- 2) rectify inaccurate personal data;
- 3) block or erase the collected personal data.

(2) A chief processor or authorised processor is required to promptly notify the data subject and third persons to whom personal data have been transmitted of the rectification of inaccurate personal data or the blocking or erasure of personal data.

(3) The obligation specified in subsection (2) of this section does not apply:

- 1) if the data subject is aware of the circumstances listed in subsection (2);
- 2) in the cases provided for in subsection 30 (1) of this Act;
- 3) if notification of the data subject would involve difficulties on a disproportionate scale.

§ 32. Data subject's right of recourse to Data Protection Inspectorate or court

A data subject has a right of recourse to the Data Protection Inspectorate or a court if the data subject finds that his or her rights are violated in the processing of personal data.

§ 33. Right of data subject to claim compensation for damage

If the rights of a data subject are violated in the processing of personal data, the data subject has the right to claim compensation for the damage caused to the data subject:

1) on the bases and pursuant to procedure provided for in the State Liability Act (RT I 2001, 47, 260; 2002, 62, 377) if the rights are violated in the course of performance of public duties or

2) on the bases and pursuant to procedure provided for in the Law of Obligations Act (RT I 2001, 81, 487; 2002, 60, 374) if the rights are violated in a private law relationship.

Chapter 8 SUPERVISION

§ 34. Supervision

(1) The Data Protection Inspectorate shall monitor compliance with this Act and legislation established on the basis thereof.

(2) The Data Protection Inspectorate may initiate supervision proceedings on the basis of a complaint or on its own initiative.

(3) In implementing its obligations arising from this Act, the Data Protection Inspectorate is independent and shall act pursuant to this Act, other Acts and legislation established on the basis thereof.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

(4) The Data Protection Inspectorate shall monitor the processing of state secrets containing personal data in cases and to the extent provided for in clause 2 (3) of this Act.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 35. Requirements for head of Data Protection Inspectorate

(1) A person who has completed higher education with sufficient legal training and management and IT administration and auditing experience may work as the head of the Data Protection Inspectorate.

(2) A person who has been convicted of an intentionally committed criminal offence or who has been released from any position or office requiring higher education due to unsuitability for continued work shall not be the head of the Data Protection Inspectorate.

(3) The head of the Data Protection Inspectorate shall not participate in the activities of political parties, hold any other remunerative position or office during his or her term of office, except for pedagogical work or research.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

(4) The Government of the Republic shall appoint the head of Data Protection Inspectorate to office for a term of five years at the proposal of the Minister of Justice after having heard the opinion of the Constitutional Committee of the Riigikogu.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 35¹. Security check of candidate for Head of Data Protection Inspectorate

(1) The candidate for Head of Data Protection Inspectorate must pass a security check before being appointed the Head of Data Protection Inspectorate, except if he or she has a valid access permit in order to access state secrets classified as “top secret”.

(2) The security check of the candidate for Head of Data Protection Inspectorate shall be performed by the Security Police Board pursuant to the procedure provided for in the Surveillance Act.

(3) In order to pass the security check, the candidate for Head of Data Protection Inspectorate shall submit a completed form for an applicant for a permit to access state secrets classified as “top secret” to the Security Police Board through the Ministry of Justice, and also written consent which permits the agency which performs security checks to obtain information concerning the person from natural and legal persons and state and local government agencies and bodies during the performance of the security check.

(4) The Security Police Board shall, within three months as of receipt of the documents specified in subsection (3) of this section, present the information gathered as a result of the security check to the Minister of Justice and shall provide an opinion concerning the compliance of the candidate for Head of Data Protection Inspectorate with the conditions for the issue of a permit for access to state secrets.

(5) In the cases where the authority of the Head of Data Protection Inspectorate has terminated prematurely, the security check of the candidate for Head of Data Protection Inspectorate shall be performed within one month as of the receipt of the documents specified in subsection (3) of this section. With the permission of the Committee for the Protection of State Secrets, the term for performing the security check may be extended by one month if circumstances specified in clause 30 (2¹) 1) or 2) of the State Secrets Act

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 35². Release from office of head of Data Protection Inspectorate

(1) The director general of the Data Protection Inspectorate may be released from office:

1) at his or her own request;

2) due to the expiry of the term of office;

- 3) for a disciplinary offence;
- 4) due to long-term incapacity for work;
- 5) upon entry into force of a judgment of conviction with regard to him or her;
- 6) if facts become evident which according to law preclude the appointment of the person as director general.

(2) The Government of the Republic shall release the head of Data Protection Inspectorate from office at the proposal of the Minister of Justice after having heard the opinion of the Constitutional Committee of the Riigikogu. The opinion of the Constitutional Committee of the Riigikogu need not be obtained if the release from office is carried out on the basis of clauses (1) 1), 2), 5) or 6). Reason shall be provided for disregarding the opinion of the Constitutional Committee of the Riigikogu.

(3) The provisions of the Public Service Act apply to the release from office of the director general of the Data Protection Inspectorate with the differences arising from this section.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 36. Functions of Data Protection Inspectorate

(1) The Data Protection Inspectorate shall:

- 1) monitor compliance with the requirements provided for in this Act;
- 2) apply administrative coercion on the bases, to the extent and pursuant to the procedure prescribed by Acts;
- 3) initiate misdemeanour proceedings, if necessary, and impose a punishment;
- 4) co-operate with international data protection supervision organisations and foreign data protection supervision authorities and other competent foreign authorities and persons;
- 5) provide recommended instructions for the implementation of this Act;
- 6) perform other functions arising from Acts.

(2) In the performance of its functions, the Data Protection Inspectorate has all the rights provided for in this Act and legislation established on the basis thereof, including the right to:

- 1) suspend the processing of personal data;
- 2) demand the rectification of inaccurate personal data;
- 3) prohibit the processing of personal data;
- 4) demand the blocking or the termination of processing of personal data (including destruction or transfer to an archives);
- 5) promptly apply, if necessary, the organisational, physical and IT security measures to protect personal data pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act (RT I 2001, 50, 283; 94, 580) in order to prevent damage to the rights and freedoms of persons;
- 6) demand relevant documents and other necessary information from persons and make copies of the documents.

(3) A competent official of the Data Protection Inspectorate has the right of unhindered access to inspect the territory or rooms of chief processors and authorised processors, the right to obtain access to the documents and equipment of chief processors and authorised processors, including recorded data, and to software used for data processing.

§ 37. Obligations of Data Protection Inspectorate

An official of the Data Protection Inspectorate is required to:

- 1) act pursuant to this Act, other Acts and legislation established on the basis thereof;
- 2) maintain the confidentiality of restricted information and personal data which become known to him or her in the performance of his or her duties over an unspecified term;
- 3) present identification at the request of the person being inspected;

- 4) prepare an inspection report on the results of supervision;
- 5) in the event of violation of the personal data processing requirements, explain the nature of the violation to the chief processor or authorised processor or the representative thereof and demand termination of the violation;
- 6) in the event of violation of the personal data processing requirements, issue a precept or initiate misdemeanour proceedings.

§ 38. Term for review of complaints

- (1) The Data Protection Inspectorate shall settle a complaint within thirty days as of submission of the complaint with the Data Protection Inspectorate.
- (2) The Data Protection Inspectorate may extend the term for review of a complaint for up to sixty days in order to additionally ascertain facts necessary for settling the complaint. The complainant shall be notified of extension of the term in writing.

§ 39. Inspection report

- (1) An inspection report shall be prepared on monitoring of the compliance with the personal data processing requirements.
- (2) An inspection report shall set out:
 - 1) the given name, surname and official title of the person who prepared the report;
 - 2) the given name, surname and address of the addressee of the report or the name and postal address of a legal person;
 - 3) the content of the act (legal basis, facts established, explanations of chief processors or authorised processors or their representatives and other facts relevant to the matter);
 - 4) the time and place of preparation of the report;
 - 5) the signature of the person who prepared the report.

§ 40. Precept of Data Protection Inspectorate

- (1) In order to ensure compliance with this Act, an official of the Data Protection Inspectorate has the right to issue precepts to chief processors and authorised processors and make decisions.
- (2) Upon failure to comply with a precept specified in subsection (1) of this section, the Data Protection Inspectorate may impose a penalty payment pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act.
- (3) The upper limit for a penalty payment specified in subsection (2) of this section is 10 000 kroons.
- (3¹) If a state agency who is the processor of personal data fails to comply with the precept of the Data Protection Inspectorate within the term specified therein, the Data Protection Inspectorate shall file a protest with an administrative court pursuant to procedure provided for in the Code of Administrative Court Procedure.
(RT I 2007, 11, 53 – entered into force 18.02.2007)
- (4) The decisions and precepts of the Data Protection Inspectorate concerning suspension of the right to process personal data and termination of and prohibition on the processing of personal data shall be entered in the register of processors of personal data.

§ 41. Report of Data Protection Inspectorate on compliance with this Act

- (1) The Data Protection Inspectorate shall submit a report on compliance with this Act to the Constitutional Committee of the Riigikogu and to the Chancellor of Justice by 1 December each year.
- (2) A report shall contain an overview of the essential circumstances relating to the compliance with and implementation of this Act.

(3) Reports shall be published on the web site of the Data Protection Inspectorate.

(4) In addition to the regular reports specified in subsection (1) of this section, the head of the Data Protection Inspectorate may submit reports to the Constitutional Committee of the Riigikogu concerning significant matters having an extensive effect or needing prompt settlement which become known in the course of supervision over compliance with this Act.
(RT I 2007, 11, 53 – entered into force 18.02.2007)

Chapter 9 LIABILITY

§ 42. Violation of requirements of this Act

(1) Failure to comply with the obligation to register the processing of sensitive personal data, the obligation to forward personal data to foreign countries provided in § 28 of this Act and the obligation to notify the data subject provided in §§ 12 and 15 of this Act is punishable by a fine of up to 300 fine units.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

(2) The same act, if committed by a legal person, is punishable by a fine of up to 500 000 kroons.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

42¹. Violation of requirements regarding security measures to protect personal data and of personal data processing requirements

(1) Violation of the requirements regarding security measures to protect personal data or violation of other requirements for the processing of personal data prescribed in this Act if a precept issued to the person by the Data Protection Inspectorate on the basis of § 40 of this Act for the elimination of the violation is not complied with is punishable by a fine of up to 300 fine units.

(2) The same act, if committed by a legal person, is punishable by a fine of up to 500 000 kroons.

(RT I 2007, 11, 53 – entered into force 18.02.2007)

§ 42². Proceedings

(1) The provisions of the General Part of the Penal Code apply to the misdemeanours provided for in §§ 42 and 42¹ of this Act.

(2) The Technical Inspectorate shall conduct extra-judicial proceedings in the matters of misdemeanours provided for in §§ 42 and 42¹ of this Act.”

(RT I 2007, 11, 53 – entered into force 18.02.2007)

Chapter 10 IMPLEMENTING PROVISIONS

§ 43. Amendment of Databases Act

Subsection 12 (2) of the Databases Act (RT I 1997, 28, 423; 1998, 36/37, 552; 1999, 10, 155; 2000, 50, 317; 57, 373; 92, 597; 2001, 7, 17; 17, 77; 2002, 61, 375; 63, 387) is repealed.

§ 44. Amendment of Public Information Act

The Public Information Act (RT I 2000, 92, 597; 2002, 61, 375; 63, 387) is amended as follows:

1) subsections 14 (2) and (4) are amended and worded as follows:

«(2) If a person requests information which contains sensitive or private personal data concerning him or her or third persons, the holder of information shall identify the person making the request for information.»

«(4) If a state or local government official or employee requests information to perform his or her functions or duties or if a person requests personal data concerning a third person, he or she shall inform the holder of information of the basis and purpose of accessing the information.»;

2) the second sentence of subsection 23 (3) is repealed;

3) clauses 10) and 11) are added to subsection 35 (1) worded as follows:

«10) information which contains private or sensitive personal data;

11) information which contains personal data if it significantly breaches the inviolability of private life of the data subject.»;

4) clause 36 (1) 6) is amended and worded as follows:

«6) information which damages the reputation of a state or local government official, a legal person in private law performing public duties or a natural person, except sensitive or private personal data;»

5) section 37 is repealed;

6) subsections 38 (2) and (4) are amended and worded as follows:

«(2) If the grant of access to information may cause the disclosure of restricted information, it shall be ensured that only the part of the information or document to which restrictions on access do not apply may be accessed.»

«(4) The head of an agency may decide to grant access to information classified as internal to persons outside the agency if this does not damage the interests of the state or a local government.»;

7) section 39 is amended and worded as follows:

«§ 39. Access to information which contains personal data

(1) A holder of information shall grant access to personal data in its possession upon the existence of a basis provided for in the Personal Data Protection Act pursuant to the procedure provided for in this Act.

(2) A holder of information is required to maintain records concerning to whom, for what purpose, when, in which manner and which information classified as internal which contains personal data is released.

(3) In order to ascertain the truth in criminal proceedings and ensure the security of persons, a competent official conducting an investigation or state supervision may grant access to information classified as internal which contains personal data. If compliance with a restriction on access may endanger the life, health or property of other persons, the restricted information shall be promptly disclosed in a manner provided for in subsection 30 (4) of this Act.»;

8) subsections 40 (1) and (3) are amended and worded as follows:

«(1) A restriction on access to information intended for internal use applies as of the preparation or receipt of the documents for as long as is necessary, but not for longer than five years. The head of an agency may extend the term by up to five years if the reason for establishment of the restriction on access continues to exist.»

«(3) A restriction on access to information classified as internal which contains private personal data applies for 75 years as of the receipt or documentation thereof or for 30 years as of the death of the person or, if it is impossible to establish death, for 110 years as of the birth of the person.»;

9) subsection 41 (2) is amended and worded as follows:

«(2) The person who prepares a document classified as information intended for internal use shall make a notation “*ASUTUSESISESEKS KASUTAMISEKS*” [“FOR INTERNAL

USE”] in capital letters on the document or file of documents, if the medium enables this, or use the corresponding abbreviation *AK*. The name of the holder of information, the basis of the restriction on access, the final date for application of the restriction on access and the date on which the notation is made shall be added to the notation.”;

10) clause 6) is added to § 47 worded as follows:

«6) the clearly expressed request of the person filing the challenge.”;

11) clause 51 (1) 8) is amended and worded as follows:

«8) has failed to establish restrictions on access to information provided by law;”;

12) subsection 54¹ (1) is amended and worded as follows:

«(1) Knowing release of incorrect public information or knowing disclosure or release of information intended for internal use or failure to comply with a precept of the Data Protection Inspectorate is punishable by a fine of up to 300 fine units.

§ 45. Registration of sensitive personal data pursuant to earlier Act

The registration of processing of sensitive personal data pursuant to the Personal Data Protection Act (RT I 1996, 48, 944; 1998, 59, 941; 111, 1833; 2000, 50, 317; 92, 597; 104, 685; 2001, 50, 283; 2002, 61, 375; 63, 387) is valid within three years after the entry into force of this Act.

§ 46. Consent for processing of personal data granted before entry force of this Act

(1) A consent for the processing of personal data granted before the entry force of this Act is deemed to be valid if the consent complies with the requirements of the Act which was in force at the time of grant of the consent.

(2) Chief processors and authorised processors shall notify a data subject, at the request of the data subject, of termination of processing and rectification, blocking, and erasure of personal data and of the conditions for access to personal data within ten working days.

§ 47. Repeal of previous Personal Data Protection Act

The Personal Data Protection Act (RT I 1996, 48, 944; 1998, 59, 941; 111, 1833; 2000, 50, 317; 92, 597; 104, 685; 2001, 50, 283; 2002, 61, 375; 63, 387) is repealed.

§ 48. Introduction of register of processors of personal data

The register of processors of personal data shall be introduced as of 1 July 2004. Until introduction of the register, applications specified in subsection 25 (1) of this Act shall be submitted to the Data Protection Inspectorate on paper. Chief processors who have commenced the processing of personal data before 1 July 2004 shall comply with the notification obligation by 31 October 2004.

§ 49. Entry into force of the Act

(1) This Act enters into force on 1 October 2003.

(2) Chapter 4 and subsection 26 (4) of this Act enter into force on 1 July 2004.

(3) Subsection 28 (2) of this Act becomes invalid and subsections 28 (3) and (5) enter into force upon Estonia's accession to the European Union.

¹ RT = *Riigi Teataja* = *State Gazette*