Personal Data Protection Act[1]

Passed 15.02.2007
RT I 2007, 24, 127
Entry into force 01.01.2008

Chapter 1 GENERAL PROVISIONS

§ 1. Scope of application and purpose of Act

(1) The aim of this Act is to protect the fundamental rights and freedoms of natural persons upon processing of personal data, above all the right to inviolability of private life.

(2) This Act provides for:

1) the conditions and procedure for processing of personal data;

2) the procedure for the exercise of state supervision and administrative supervision upon processing of personal data;

[RT I, 06.01.2016, 1 - entry into force 16.01.2016]

3) liability for the violation of the requirements for processing of personal data.

§ 2. Application of Act

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

1) processing of personal data by natural persons for personal purposes;

2) transmission of personal data through the Estonian territory without any other processing of such data in Estonia;

(2) This Act applies to criminal proceedings and court procedure with the specifications provided by procedural law.

(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).

§ 3. Application of Administrative Procedure Act

The provisions of the Administrative Procedure Act 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 any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist.

(2) 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 on the state of health or disability;

4) data on genetic information;

5) biometric data (above all fingerprints, palm prints, eye iris images and genetic data);

6) information on sex life;

7) information on trade union membership;

8) information concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter.

§ 5. Processing of personal data

Processing of personal data is any act performed with personal data, including the collection, recording, organisation, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage, combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used.

§ 6. Principles of processing personal data

Upon processing of personal data, a processor of personal data is required to adhere to the following principles:

1) principle of legality - personal data shall be collected only in an honest and legal manner;

2) principle of purposefulness - personal data shall be collected only for the achievement of determined and lawful objectives, and they shall not be processed in a manner not conforming to the objectives of data processing;

3) principle of minimalism - personal data shall be collected only to the extent necessary for the achievement of determined purposes;

4) principle of restricted use - personal data shall be used for other purposes only with the consent of the data subject or with the permission of a competent authority;

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

6) principle of security - security measures shall be applied in order to protect personal data from involuntary or unauthorised processing, disclosure or destruction;

7) principle of individual participation - the data subject shall be notified of data collected concerning him or her, the data subject shall be granted access to the data concerning him or her and the data subject has the right to demand the correction of inaccurate or misleading data.

§ 7. Processor of personal data

(1) A processor of personal data is a natural or legal person, a branch of a foreign company or a state or local government agency who processes personal data or on whose assignment personal data are processed.

(2) A processor of personal data 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 communication of personal data to third persons.

(3) A processor of personal data (hereinafter *chief processor*) may authorise, by an administrative act or contract, another person or agency (hereinafter *authorised processor*) to process personal data, unless otherwise prescribed by an Act or regulation.

(4) The chief processor shall provide the authorised processor with mandatory instructions for processing personal data and shall be responsible for the authorised processor's compliance with the personal data processing requirements. The chief processor shall determine the requirements specified in subsection (2) of this section for the authorised processor.

(5) The authorised processor may delegate the task of processing personal data to another person only with the written consent of the chief processor, provided that this does not exceed the limits of the authority of the authorised processor.

(6) A processor of personal data operating outside of the European Union who uses equipment located in Estonia for processing personal data is required to appoint a representative located in Estonia, except in the case specified in clause 2 (1) 2) of this Act.

§ 8. Data subject

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

§ 9. Third person

A third person is a natural or legal person, a branch of a foreign company or a state or local government agency who is not:

1) the processor of the personal data in question;

2) a data subject;

3) a natural person who processes personal data in the subordination of a processor of personal data.

Chapter 2PERMISSION FOR PROCESSING PERSONAL DATA

§ 10. Permission for processing personal data

(1) Processing of personal data is permitted only with the consent of the data subject unless otherwise provided by law.

(2) An administrative authority shall process personal data only in the course of performance of public duties in order to perform obligations prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission.

(3) The conditions of and procedure for processing of personal data as provided for in subsection 2 (3) of this Act shall be established by a regulation of the Government of the Republic.

§ 11. Disclosure of personal data

(1) If a data subject has disclosed his or her personal data, has given the consent specified in § 12 of this Act for the disclosure thereof or if such personal data have been disclosed on the basis of law, including subsection (2) of this section, then other sections of this Act do not apply to the processing of the personal data.

(2) Personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, if there is predominant public interest therefore and this is in accordance with the principles of journalism ethics. Disclosure of data shall not cause excessive damage to the rights of a data subject.

(3) A data subject has the right to demand, at all times, that the person disclosing his or her personal data terminate the disclosure, unless such disclosure is carried out based on law or pursuant to subsection (2) of this section and further disclosure does not excessively damage the rights of the data subject. A demand for the termination of disclosure of personal data shall not be made to a person disclosing personal data with regard to data carriers over which the person disclosing the personal data has no control at the time such demand is made.

(4) A data subject has the right to demand, at all times, that the person processing disclosed personal data discontinue such activity unless otherwise provided by law and provided that this is technically possible and does not result in disproportionately high costs.

(5) In addition to the provisions of subsections (3) and (4) of this section, a data subject has the right to make the demands provided in §§ 21-23 of this Act.

(6) Processing of personal data intended to be communicated to third persons for assessing the creditworthiness of persons or other such purpose is permitted only if:

1) the third person has legitimate interest to process personal data;

2) the person communicating the personal data has established the legitimate interest of the third person, verified the accuracy of the data to be communicated and registered the data transmission.

(7) Collection and communication of data to third persons for the purposes specified in subsection (6) of this section is not permitted if:

1) the data in question is sensitive personal data;

2) it would excessively damage the legitimate interests of the data subject;

3) less than thirty days have passed from a violation of a contract;

4) more than three years have passed from the end of the violation of an obligation.

(8) Unless otherwise provided by law, upon the making of audio or visual recordings at a public place intended for future disclosure, the consent of the data subject shall be substituted by an obligation to notify the data subject thereof in a manner which permits the person to understand

the fact of the recording of the audio or visual images and to give the person an opportunity to prevent the recording of his or her person if he or she so wishes. The notification obligation does not apply in the case of public events, recording of which for the purposes of disclosure may be reasonably presumed.

§ 12. Consent of data subject for processing of personal data

(1) The declaration of intention of a data subject whereby the person permits the processing of his or her personal data (hereinafter *consent*) is valid only if it is based on the free will of the data subject. The consent shall clearly determine the data for the processing of which permission is given, the purpose of the processing of the data and the persons to whom communication of the data is permitted, the conditions for communicating the data to third persons and the rights of the data subject concerning further processing of his or her personal data. Silence or inactivity shall not be deemed to be a consent. Consent may be partial and conditional.

(2) Consent shall be given in a format which can be reproduced in writing unless adherence to such formality is not possible due to a specific manner of data processing. If the consent is given together with another declaration of intention, the consent of the person must be clearly distinguishable.

(3) Before obtaining a data subject's consent for the processing of personal data, the processor of personal data shall notify the data subject of the name of the processor of the personal data or his or her representative, and of the address and other contact details of the processor of the personal data. If the personal data are to be processed by the chief processor and authorised processor then the name of the chief processor and authorised processor or the representatives thereof and the address and other contact details of the chief processor and authorised processor shall be communicated or made available.

(4) For processing sensitive personal data, the person must be explained that the data to be processed is sensitive personal data and the data subject's consent shall be obtained in a format which can be reproduced in writing.

(5) A data subject has the right to prohibit, at all times, the processing of data concerning him or her for the purposes of research of consumer habits or direct marketing, and communication of data to third persons who intend to use such data for the research of consumer habits or direct marketing.

(6) The consent of a data subject shall remain valid during the lifetime of the data subject and for thirty years after the death of the data subject unless the data subject has decided otherwise.

(7) Consent may be withdrawn by the data subject at any time. Withdrawal of consent has no retroactive effect. The provisions of the General Principles of the Civil Code Act concerning declaration of intention shall additionally apply to consent.

(8) In the case of a dispute it shall be presumed that the data subject has not granted consent for the processing of his or her personal data. The burden of proof of the consent of a data subject lies on the processor of personal data.

§ 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 successor, spouse, descendant or ascendant, 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. If there are more than one successor or other persons specified in this subsection, processing of the data subject's personal data is permitted with the consent of any of them but each of the successors has the right to withdraw the consent.

(2) The consent specified in subsection (1) of this section is not required if the personal data to be processed only contains the data subject's name, sex, date of birth and death and the fact of death.

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

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

1) on the basis of law;

2) for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;

3) in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible;

4) for performance of a contract entered into with the data subject or for ensuring the performance of such contract unless the data to be processed are sensitive personal data.

(2) Communication of personal data or granting access to personal data to third persons for the purposes of processing is permitted without the consent of the data subject:

1) if the third person to whom such data are communicated processes the personal data for the purposes of performing a task prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;

2) in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible;

3) if the third person requests information obtained or created in the process of performance of public duties provided by an Act or legislation issued on the basis thereof and the data requested do not contain any sensitive personal data and access to it has not been restricted for any other reasons.

(3) Surveillance equipment transmitting or recording personal data may be used for the protection of persons or property only if this does not excessively damage the legitimate interests of the data subject and the collected data are used exclusively for the purpose for it is collected. In such case, the consent of the data subject is substituted by sufficiently clear communication of the fact of the use of the surveillance equipment and of the name and contact details of the

processor of the data. This requirement does not extend to the use of surveillance equipment by state agencies on the bases and pursuant to the procedure provided by law.

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

(1) If the source of personal data is any other than the data subject himself or herself, then after obtaining or amending of the personal data or communicating the data to third persons, the processor of the personal data must promptly inform the data subject of the categories and source of the personal data to be processed together with the information specified in subsection 12 (3) of this section.

(2) A data subject need not be informed of the processing of his or her personal data:

1) if the data subject has granted consent for the processing of his or her personal data;

2) if the data subject is aware of the circumstances specified in subsection (1) of this section;

3) if processing of the personal data is prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;

4) if informing of the data subject is impossible;

5) in the cases provided for in subsection 20 (1) of this Act.

§ 16. Processing of personal data for scientific research or official statistics needs

(1) Data concerning a data subject may be processed without the consent of the data subject for the needs of scientific research or official statistics only in coded form. Before handing over data for processing it for the needs of scientific research or official statistics, the data allowing a person to be identified shall be substituted by a code. Decoding and the possibility to decode is permitted only for the needs of additional scientific research or official statistics. The processor of the personal data shall appoint a specific person who has access to the information allowing decoding.

(2) Processing of data concerning a data subject without the person's consent for scientific research or official statistics purposes in a format which enables identification of the data subject is permitted only if, after removal of the data enabling identification, the goals of data processing would not be achievable or achievement thereof would be unreasonably difficult. In such case, the personal data of a data subject may be processed without the person's consent only if the person carrying out the scientific research finds that there is a predominant public interest for such processing and the volume of the obligations of the data subject is not changed on the basis of the processed personal data and the rights of the data subject are not excessively damaged in any other manner.

(3) Processing of personal data for scientific research or official statistics purposes without the consent of the data subject is permitted if the processor of the personal data has taken sufficient organisational, physical and information technology security measures for the protection of the personal data, has registered the processing of sensitive personal data and the Data Protection Inspectorate has verified, before the commencement of the processing of the personal data,

compliance with the requirements set out in this section and, if an ethics committee has been founded based on law in the corresponding area, has also heard the opinion of such committee.

(4) Collected personal data may be processed for the purposes of scientific research or official statistics regardless of the purpose for which the personal data were initially collected. Personal data collected for scientific research or official statistics may be stored in coded form for the purposes of using it later for scientific research or official statistics.

§ 17. Automated decisions

(1) The making of a decision by a data processing system without the participation of the data subject (hereinafter *automated decision*) for assessment of the character, abilities or other characteristics of the data subject which results in legal consequences to the data subject or significantly affects the data subject is prohibited except in the following cases:

1) the automated decision concerning a data subject is made in the process of entry into or performance of a contract, provided that the request of the data subject for entry into or performance of the contract will be satisfied or the data subject will be given an opportunity to file an objection against the decision in order to protect his or her legitimate interests;

2) making of the automated decision is prescribed by law if the law provides measures for the protection of the legitimate interests of the data subject.

(2) Before making an automated decision, the data subject shall be informed, in an understandable manner, of the process of and conditions for data processing based on which the automated decision will be made.

§ 18. Transfer of personal data to foreign countries

(1) Transfer of personal data from Estonia is permitted only to a country which has a sufficient level of data protection.

(2) Transfer of personal data is permitted to the Member States of the European Union and the States party to the Agreement of the of the European Economic Area, and to countries whose level of data protection has been evaluated as sufficient by the European Commission. Transfer of personal data is not permitted to a country whose level of data protection has been evaluated as insufficient by the European Commission.

(3) Personal data may be transferred to a foreign country which does not meet the conditions provided in subsection (1) of this section only with the permission of the Data Protection Inspectorate if:

1) the chief processor guarantees, for that specific event, the protection of the rights and inviolability of the private life of the data subject in such country;

2) sufficient level of data protection is guaranteed in such country for that specific case of data transfer. In evaluating the level of data protection, the circumstances related to the transfer of personal data shall be taken into account, including the categories of the data, the objectives and duration of processing, the country of destination and final destination of the data, and the law in force in that country.

(4) The Data Protection Inspectorate shall inform the European Commission of the grant of the permission on the basis of subsection (3) of this section.

(5) Personal data may be transferred to a foreign country which does not meet the conditions provided in subsection (1) of this section without the permission of the Data Protection Inspectorate if:

1) the data subject has granted permission to this effect pursuant to § 12 of this Act;

2) the personal data are transferred in the cases provided for in clauses 14 (2) 2) and 3) of this Act.

Chapter 3RIGHTS OF DATA SUBJECT

§ 19. Right of data subjects to obtain information and personal data concerning them

(1) At the request of a data subject, a processor of personal data shall communicate the following to the data subject:

1) the personal data concerning the data subject;

2) the purposes of processing of personal data;

3) the categories and source of personal data;

4) third persons or categories thereof to whom transfer of the personal data is permitted;

5) third persons to whom the personal data of the data subject have been transferred;

6) the name of the processor of the personal data or representative thereof and the address and other contact details of the processor of the personal data.

(2) A data subject has the right to obtain personal data relating to him or her from the processor of personal data. Where possible, personal data are issued in the manner requested by the data subject. The processor of personal data may demand a fee of up to 0.19 euros per page for release of personal data on paper starting from the twenty-first page, unless a state fee for the release of information is prescribed by law.

[RT I, 30.12.2010, 2 - entry into force 01.01.2011]

(3) The processor of personal data 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 the corresponding request. Derogations from the procedure for provision of information concerning personal data and release of personal data to a data subject may be prescribed by an Act.

(4) After the death of a data subject, his or her successor, spouse, descendant or ascendant, brother or sister shall have the rights concerning the personal data of the data subject provided by this Chapter.

§ 20. Restrictions to right to receive information and personal data

(1) The rights of a data subject to receive information and personal data concerning him or her upon the processing of the personal data shall be restricted if this may:

1) damage rights and freedoms of other persons;

2) endanger the protection of the confidentiality of filiation of a child;

3) hinder the prevention of a criminal offence or apprehension of a criminal offender;

4) complicate the ascertainment of the truth in a criminal proceeding.

(2) A processor of personal data shall inform a data subject of the decision to refuse to release information or personal data. If personal data are processed by the authorised processor, then the chief processor shall decide on the refusal to release data or information.

§ 21. Right of data subject to demand termination of processing of personal data and correction, closure and deletion of personal data

(1) A data subject has the right to demand the correction of inaccurate personal data concerning the data subject from the processor of his or her personal data.

(2) If processing of personal data is not permitted on the basis of law, a data subject has the right to demand:

1) termination of the processing of the personal data;

2) termination of the disclosure or enabling access to the personal data;

3) deletion or closure of the collected personal data.

(3) A processor of personal data shall immediately perform the act provided in subsections (1) or (2) at the demand of a data subject unless the circumstances provided in subsection 20 (1) of this Act exist or the data subject's demand is unjustified. The processor of personal data shall notify the data subject of the satisfaction of his or her demand. Reasons for denial shall be provided to the data subject.

§ 22. 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, unless a different procedure for contestation is provided by law.

§ 23. Right of data subject to demand compensation for damage

If the rights of a data subject have been violated upon processing of personal data, the data subject has the right to demand compensation for the damage caused to him or her:

1) on the basis and pursuant to the procedure provided by the State Liability Act if the rights were violated in the process of performance of a public duty, or

2) on the basis and pursuant to the procedure provided by the Law of Obligations Act if the rights were violated in a private law relationship.

Chapter 4REQUIREMENTS FOR PROCESSING PERSONAL DATA AND SECURITY MEASURES FOR PROTECTION OF PERSONAL DATA

§ 24. Personal data processing requirements

Upon processing of personal data, a processor of personal data is required to:

1) immediately delete or close personal data which are not necessary for achieving the purposes thereof, unless otherwise provided by law;

2) guarantee that the personal data are accurate, and if necessary for achievement of the purposes, kept up to date;

3) ensure that incomplete and inaccurate personal data are closed, and necessary measures are immediately taken for amendment or rectification thereof;

4) ensure that inaccurate data are stored with a notation concerning their period of use together with accurate data;

5) ensure that personal data which are contested on the basis of accuracy are closed until the accuracy of the data is verified or the accurate data are determined;

6) upon rectification of personal data, inform the third persons who provided the personal data or to whom the personal data were forwarded if this is technically possible and does not result in disproportionate costs.

§ 25. Organisational, physical and information technology security measures for protection of personal data

(1) A processor of personal data is required to take organisational, physical and information technology security measures to protect personal data:

1) against accidental or intentional unauthorised alteration of the data, in the part of the integrity of data;

2) against accidental or intentional destruction and prevention of access to the data by entitled persons, in the part of the availability of data;

3) against unauthorised processing, in the part of confidentiality of the data.

(2) Upon processing of personal data, the processor of personal data is required to:

1) prevent access of unauthorised persons to equipment used for processing personal data;

2) prevent unauthorised reading, copying and alteration of data within the data processing system, and unauthorised transfer of data carriers;

3) prevent unauthorised recording, alteration and deleting of personal data and to ensure that it be subsequently possible to determine when, by whom and which personal data were recorded, altered or deleted or when, by whom and which data were accessed in the data processing system;

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 to which the person is authorised;

5) ensure the existence of information concerning the transmission of data: when, to whom and which personal data were transmitted and ensure the preservation of such data in an unaltered state;

6) ensure that unauthorised reading, copying, alteration or erasure is not carried out in the course of transmission of personal data via data communication equipment, and upon transportation of data carriers;

7) organise the work of enterprises, agencies or organisations in a manner that allows compliance with data protection requirements.

(3) A processor of personal data is required to keep account of the equipment and software under the control thereof used for processing of personal data, and record the following data:

1) the name, type, location and name of the producer of the equipment;

2) the name, version and name of the producer of the software, and the contact details of the producer.

§ 26. Requirements for persons processing personal data

(1) A natural person processing personal data in the subordination of a processor of personal data is required to process the data for the purposes and under the conditions permitted by this Act, and in adherence to the instructions and orders of the chief processor.

(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) A processor of personal data is required to guarantee training in the area of protection of personal data to persons engaged in the processing personal data in the subordination thereof.

Chapter 5REGISTRATION OF PROCESSING SENSITIVE PERSONAL DATA

§ 27. Obligation to register processing of sensitive personal data

(1) If a processor of personal data has not appointed a person responsible for the protection of personal data provided in § 30 of this Act, the processor of personal data is required to register the processing of sensitive personal data with the Data Protection Inspectorate. If personal data are processed by an authorised processor then the applications provided by this Chapter shall be submitted by the chief processor.

(2) The economic activity of a person shall not be registered and a person shall not be issued an activity licence or licence in areas of activity which involve processing of sensitive personal data if the person has not registered the processing of sensitive personal data with the Data Protection Inspectorate or appointed a person responsible for data protection.

(3) Processing of sensitive personal data is registered for a period of five years. A processor of personal data is required to submit a new application for registration not later than three months prior to the expiry of the term for registration.

(4) Processing of sensitive personal data is prohibited if:

1) the Data Protection Inspectorate has not registered the processing of sensitive personal data, except in the case specified in subsection 30 (1) of this Act;

2) the term for processing sensitive personal data has expired;

3) 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 are no legal grounds for processing;

2) the conditions for processing do not meet the requirements provided for in this Act, another Act or legislation established on the basis thereof;

3) the organisational, physical and information technology security measures applied for the protection of personal data do not ensure compliance with the requirements provided for in § 25 of this Act.

§ 28. Registration application

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

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

1) the name, registry or personal identification code, place of business, seat or residence and other contact details of the processor of the personal data, including the authorised processor;

2) a reference to the legal grounds of the processing of personal data;

3) the purposes of processing of personal data;

4) the categories of personal data;

5) the categories of persons whose data are processed;

6) the sources of personal data;

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

8) place or places of processing of personal data;

9) the conditions for transfer of personal data to foreign states;

10) a detailed description of the organisational, physical and information technology security measures for the protection of personal data specified in subsection 25 (2) of this Act;

11) the opinion of the ethics committee provided on the basis of subsection 16 (3) of this Act, if this exists.

§ 29. Processing of registration application

(1) The Data Protection Inspectorate shall decide on the registration or refusal to register processing of sensitive personal data within 20 working days after the date of submission of the registration application.

(2) The Data Protection Inspectorate may inspect, at the site, readiness for processing sensitive personal data. In such case, the term for resolving the registration application is extended by ten working days. As a result of the inspection, the Data Protection Inspectorate may give recommendations for the application and improvement of the organisational, physical and information technology security measures for the protection of personal data.

(3) The right of a processor of personal data to process sensitive personal data is created as of the date determined by the decision provided in subsection (1) of this section. If the decision does not specify a date, the processor of personal data has the right to commence the

processing of sensitive personal data as of the day following the date of entry of the processor in the register of processors of personal data.

(4) A decision to register processing of sensitive personal data is deemed to be delivered to the chief processor at the time such decision is published on the website of the Data Protection Inspectorate. A notation is made in the register of processors of personal data concerning a decision on refusal of registration and such decision is communicated to the applicant by delivering the decision to the applicant.

(5) A processor of personal data is required to register the amendment of data subject to entry in the register of processors of personal data with the Data Protection Inspectorate. The provisions concerning the terms for registration of the processing of personal data apply to the registration of amendment of data.

§ 30. Person responsible for protection of personal data

(1) A processor of personal data need not register processing of sensitive personal data with the Data Protection Inspectorate if the processor has appointed a person responsible for the protection of personal data. The Data Protection Inspectorate shall be immediately informed of the appointment of a person responsible for the protection of personal data and termination of such person's authority. Upon appointment of a person responsible for the protection of personal data, the Data Protection Inspectorate shall be informed of the person's name and contact details.

(2) A person responsible for the protection of personal data is independent in his or her activities from the processor of personal data and shall monitor the compliance of the processor of personal data upon processing of personal data with this Act and other legislation.

(3) A person responsible for the protection of personal data shall keep a register of data processing performed by the processor of personal data which shall contain the data specified in clauses 28 (2) 1)–7) of this Act.

(4) If a person responsible for the protection of personal data has informed the processor of personal data of a violation discovered upon the processing of personal data and the processor of personal data does not immediately take measures to terminate the violation then the person responsible for the protection of personal data shall immediately inform the Data Protection Inspectorate of the discovered violation.

(5) If a person responsible for the protection of personal data is in doubt as to which requirements are applicable to the processing of personal data or which security measures must be applied upon processing of personal data then the person must obtain the opinion of the Data Protection Inspectorate in such matter before the processing of personal data is commenced.

§ 31. Register of processors of personal data and persons responsible for protection of personal data

(1) The register of processors of personal data and persons responsible for the protection of personal data is a database maintained by the Data Protection Inspectorate which contains data

on the registration of sensitive personal data and appointment of persons responsible for the protection of personal data.

(2) Information submitted to the Data Protection Inspectorate concerning organisational, physical and information technology security measures for the protection of personal data, and information concerning the conditions for the closure, deletion and destruction of personal data is deemed to be information intended for internal use.

(3) The register is accessible to the public through the website of the Data Protection Inspectorate, except for the data specified in subsection (2) of this section and the data concerning the processing of personal data by security authorities.

(4) Data entered in the register are informative. Entries concerning the registration of sensitive personal data have legal effect.

(5) The procedure for maintaining the register specified in subsection (1) of this section shall be established by the Government of the Republic.

Chapter 6SUPERVISION

§ 32. Supervision

(1) State and administrative supervision over compliance with the requirements provided for in this Act and legislation established on the basis thereof shall be exercised by the Data Protection Inspectorate.

[RT I, 13.03.2014, 4 - entry into force 01.07.2014]

(2) 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.

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

§ 32[1]. Special state supervision measures

In order to exercise state supervision provided for in this Act, the Data Protection Inspectorate may apply the specific state supervision measures provided for in §§ 30, 31, 32, 49, 50 and 51 of the Law Enforcement Act on the basis of and pursuant to the procedure provided for in the Law Enforcement Act.

[RT I, 06.01.2016, 1 - entry into force 16.01.2016]

§ 32[2]. Specifications for exercise of state supervision

The Data Protection Inspectorate may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens used in the public electronic communications network, except for the data relating to the fact of transmission of messages.

[RT I, 13.03.2014, 4 - entry into force 01.07.2014]

§ 32[3]. Specifications for administrative supervision

Upon exercise of administrative supervision, competent officials of the Data Protection Inspectorate have the right to enter, without hindrance, the premises or territory of a processor of personal data, demand relevant documents and other necessary information from persons, make copies of documents and access the equipment of a processor of personal data as well as the recorded data and the software used for data processing.

[RT I, 13.03.2014, 4 - entry into force 01.07.2014]

§ 33. Tasks of Data Protection Inspectorate

(1) The Data Protection Inspectorate shall:

1) monitor compliance with the requirements provided by this Act;

2) apply administrative coercion on the bases, to the extent and pursuant to the procedure prescribed by Acts;

3) initiate misdemeanour proceedings where necessary and impose punishments;

4) co-operate with international data protection supervision organisations and foreign data protection supervision authorities and other competent foreign authorities and persons;

5) give instructions of advisory nature for application of this Act;

6) perform other duties provided by Acts.

(2) In performing its functions, the Data Protection Inspectorate has all the rights provided by this Act and legislation issued 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 closure or termination of processing of personal data, including destruction or forwarding to an archive;

5) where necessary, immediately apply, in order to prevent the damage to the rights and freedoms of persons, organisational, physical or information technology security measures for the protection of personal data pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act, unless the personal data are processed by a state agency.

6) [repealed - RT I, 13.03.2014, 4 - entry into force 01.07.2014]

(3) The provisions of clauses (2) 1), 3) and 4) of this section apply with regard to a state agency only if non-application would result in significant damage to the rights of the data subject.

(4) [Repealed - RT I, 13.03.2014, 4 - entry into force 01.07.2014]

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

§ 34. Requirements set for head of Data Protection Inspectorate

(1) A person with management skills and higher education who has sufficient expertise in the legal regulation of the protection of personal data and in information systems may be employed as the head of the Data Protection Inspectorate.

(2) A person who has been convicted of an intentionally committed criminal offence or 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 in the field of pedagogical work or research.

§ 35. 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 or if at the time of becoming a candidate he or she holds a position which provides the right by virtue of office to access all classifications of state secrets.

(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 Security Authorities 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 shall sign a 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 responsible for the area 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 33 (4) 1) or 2) of the State Secrets and Classified Information of Foreign States Act become evident or a circumstance specified in clause 3) or 4) may become evident within one month.

(6) Based on the information gathered throughout the security checks, a candidate for the position of the head of the Data Protection Inspectorate may be appointed to office within nine months as of the forwarding of the information gathered throughout the security checks to the minister responsible for the area by the Estonian Internal Security Service. A candidate for the

position of the head of the Data Protection Inspectorate may be appointed to office later than the above term after passing a new security check.

§ 36. Appointment and release of head of Data Protection Inspectorate from office

(1) 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 responsible for the area after having heard the opinion of the Constitutional Committee of the *Riigikogu*.

(2) The Director General of the Data Protection Inspectorate may be released from office:

1) at his or her own request;

2) due to expiry of term of office;

3) for a disciplinary offence;

4) due to long-term incapacity for work;

5) upon the 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 a director general.

(3) The Government of the Republic shall release the head of the Data Protection Inspectorate from office on the proposal of the minister responsible for the area after considering the opinion of the Constitutional Committee of the *Riigikogu*. The position of the Constitutional Committee need not be asked if the head is released from office on the basis of clauses (2) 1), 2), 5) or 6). If the opinion of the Constitutional Committee of the *Riigikogu* is not taken into account, reasons shall be provided therefor.

§ 37. Obligations of Data Protection Inspectorate

[Repealed - RT I, 13.03.2014, 4 - entry into force 01.07.2014]

§ 38. Term for review of complaints

(1) The Data Protection Inspectorate shall settle a complaint within thirty days after the date of filing the complaint with the Data Protection Inspectorate.

(2) The Data Protection Inspectorate may extend the term for review of a complaint by up to sixty days in order to additionally clarify circumstances relevant to the settling of the complaint. A person filing the complaint shall be notified of extension of the term in writing.

§ 39. Inspection report

(1) An inspection report shall be prepared concerning an inspection of the conformity to the requirements for processing of personal data.

(2) An inspection report shall set out:

1) the given name, surname and official title of the person who prepares 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 inspection act (legal basis, established facts, explanations of the chief processor or authorised processor or representative thereof and other circumstances relevant to the matter);

4) the time and place of preparation of the report;

5) the signature of the person who prepares the report.

§ 40. Precept of Data Protection Inspectorate

(1) Officials of the Data Protection Inspectorate have the right to issue precepts to processors of personal data and adopt decisions for the purposes of ensuring compliance with this Act.

(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. The upper limit for a penalty payment is 9600 euros. Penalty payment shall not be imposed on state agencies.

[RT I 2010, 22, 108 - entry into force 01.01.2011]

(3) The decisions and precepts of the Data Protection Inspectorate concerning the suspension, termination and prohibition of the right to process personal data shall be entered in the register of processors of personal data.

(4) 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.

§ 40[1]. Application of Data Protection Inspectorate for organisation of supervisory control

(1) If a processor of personal data fails to comply with a precept of the Data Protection Inspectorate, the Data Protection Inspectorate may address a superior agency, person or body of the processor of personal data for organisation of supervisory control or commencement of disciplinary proceedings against an official.

(2) A person exercising supervisory control or a person with the right to commence disciplinary proceedings is required to review an application within one month as of receipt thereof and submit a reasoned opinion to the Data Protection Inspectorate. Upon supervisory control or commencement of disciplinary proceedings, the person exercising supervisory control or the person with the right to commence disciplinary proceedings is required to immediately notify the Data Protection Inspectorate of the results thereof.

[RT I, 12.07.2014, 1 - entry into force 01.01.2015]

§ 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 Legal Chancellor by 1 April each year.

(2) The report shall provide an overview of the most important facts related to the compliance and application of this Act during the preceding calendar year.

(3) Reports shall be published on the website 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 concerning significant matters which have an extensive effect or need prompt settlement which become known in the course of supervision

over compliance with this Act to the Constitutional Committee of the *Riigikogu* and the Legal Chancellor.

[RT I, 12.07.2014, 1 - entry into force 01.01.2015]

Chapter 7LIABILITY

§ 42. Violation of personal data processing requirements

[RT I, 12.07.2014, 1 - entry into force 01.01.2015]

(1) Violation of the obligation to register the processing of sensitive personal data, violation of the requirements regarding security measures to protect personal data or violation of other requirements for the processing of personal data.

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 32,000 euros.

[RT I 2010, 22, 108 - entry into force 01.01.2011]

(3) [Repealed – RT I 12.07, 2014, 1 - entry into force 01.01.2015]

(4) [Repealed – RT I 12.07, 2014, 1 - entry into force 01.01.2015]

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

[Repealed – RT I 12.07, 2014, 1 - entry into force 01.01.2015]

§ 44. Proceedings

Extra-judicial proceedings concerning the misdemeanour provided for in § 42 of this Act shall be conducted by the Data Protection Inspectorate.

[RT I, 12.07.2014, 1 - entry into force 01.01.2015]

Chapter 8IMPLEMENTING PROVISIONS

§ 45. Implementation of Act

Processing of the personal data collected before the entry into force of this Act shall be brought into conformity with this Act within one year after the date of entry into force of this Act.

§ 46. Repeal of Personal Data Protection Act

The Personal Data Protection Act is repealed.

§ 47. – § 53. [Omitted from this text]

§ 54. Amendment of Insurance Activities Act

[Omitted - RT I 2007, 68, 421 - entry into force 20.12.2007]

§ 55. – § 56. [Omitted from this text]

§ 57. Amendment of Motor Third Party Liability Insurance Act

[Omitted - RT I 2007, 68, 421 - entry into force 20.12.2007]

§ 58. – § 72. [Omitted from this text]

§ 73. Entry into force of Act

This Act enters into force on 1 January 2008.

[1]Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.95, p. 31–50).