Issuer:	Riigikogu
Type:	act
In force from:	15.01.2019
In force until:	In force
Translation published:	23.01.2019

Personal Data Protection Act[1]

Passed 12.12.2018

Chapter 1
GENERAL PROVISIONS

§ 1. Scope of regulation of Act

(1) This Act regulates:
1) protection of natural persons upon processing of personal data to the extent in which it elaborates and supplements the provisions contained in Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016, pp. 1-88);
2) protection of natural persons upon processing of personal data by law enforcement authorities in the prevention, detection and proceedings of offences and execution of punishments.

(2) This Act provides for:
1) standards for implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council;
2) standards for transposition of Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 04.05.2016, pp. 89-131);
3) procedure for exercise of state supervision over compliance with the requirements for the processing of personal data;
4) liability for the violation of the requirements for processing of personal data.

§ 2. Specifications for application of Regulation (EU) 2016/679 of the European Parliament and of the Council

This Act and Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply to:
1) offence proceedings and judicial proceedings with the specifications provided by procedural law;
2) constitutional institutions insofar as this concerns the performance of their constitutional duties and is not regulated in the specific Acts that concern them.

§ 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.

Chapter 2
SPECIFIC GROUNDS FOR PROCESSING OF PERSONAL DATA

§ 4. Processing of personal data for journalistic purposes

Personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, in particular disclosed in the media, if there is public interest therefor and this is in accordance with the principles of journalism ethics. Disclosure of personal data must not cause excessive damage to the rights of any data subjects.

§ 5. Processing of personal data for academic, artistic and literary expression

Personal data may be processed without the consent of the data subject for the purpose of academic, artistic and literary expression, in particular disclosed if this does not cause excessive damage to the rights of the data subject.

§ 6. Processing of personal data for needs of scientific and historical research and official statistics

(1) Personal data may be processed without the consent of the data subject for the needs of scientific and historical research and official statistic, in particular in a pseudonymised format or a format which provides equivalent level of protection. Prior to transmission of personal data for processing for the needs of scientific and historical research or official statistics, personal data shall be replaced by pseudonymised data or data in a format which provides equivalent level of data protection.

(2) Depseudonymisation or any other method by which the data not enabling identification of persons are changed again into the data which enable identification of persons are only permitted for the needs of additional scientific and historical research or official statistics. Processors of personal data shall designate a person identified by name who has access to the information allowing pseudonymisation.

(3) Processing of data concerning any data subjects for the needs of scientific and historical research or official statistics without the consent of the data subject in a format which enables identification of the data subject is permitted only in the case the following conditions are met:
1) the purposes of data processing can no longer be achieved after removal of the data enabling identification or it would be unreasonably difficult to achieve these purposes;
2) there is overriding public interest for it in the estimation of the persons conducting scientific and historical research or compiling official statistics;
3) the scope of obligations of the data subject is not changed based on the processed personal data or the rights of the data subject are not excessively damaged in any other manner.

(4) If scientific and historical research is based on special categories of personal data, the ethics committee of the area concerned shall first verify compliance with the terms and conditions provided for in this section. If there is no ethics committee in the scientific area, the compliance with the requirements shall be verified by the Estonian Data Protection Inspectorate. With regard to any personal data retained at the National Archives, the National Archives shall have the rights of the ethics committee.

(5) For the purposes of this Act, scientific research is deemed to also include any analyses and studies by executive power which are carried out for the purposes of policy development. In order to prepare these, the executive power has the rights to make queries to databases of another controller or processor and process the personal data received. The Estonian Data Protection Inspectorate shall verify, prior to the beginning of the specified processing of personal data, compliance with the terms and conditions provided for in this section, except in the case the objectives of the studies conducted for policy development and the scope of processing of personal data derive from legislation.

(6) Where personal data are processed for the purpose of scientific and historical research or official statistics, the controller or processor may restrict the rights of data subjects provided for in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 of the European Parliament and of the Council insofar as the exercise of these rights is likely to make the achievement of the objectives of the scientific and historical research or official statistics impossible or impedes it to a significant extent.

§ 7. Processing of personal data for archiving in public interest

(1) If personal data are processed for the purpose of archiving in the public interest, the controller or processor may restrict the rights of the data subject provided for in Articles 15, 16 and 18-21 of Regulation (EU) 2016/679 of the European Parliament and of the Council insofar as the exercise of these rights is likely to make the achievement of the purpose of archiving in the public interest impossible or impedes it to a significant extent.

(2) The rights of data subjects specified in subsection (1) of this section may be restricted in order not to endanger the condition, authenticity, reliability, integrity and usability of the records.

Chapter 3
OTHER CASES OF PROCESSING PERSONAL DATA

§ 8. Processing of children's personal data for provision of information society services

(1) If Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council applies in connection with provision of information society services directly to a child, processing of the child's personal data is permitted only in the case the child is at least 13 years old.

(2) If the child is below the age of 13 years, processing of personal data is permitted only in the case and to the extent for which consent has been given by the legal representative of the child.

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

(1) The consent of a data subject shall remain valid during the lifetime of the data subject and for 10 years after the death of the data subject, unless the data subject decided otherwise. If the data subject died as a minor, his or her consent shall be valid for the term of 20 years after the death of the data subject.

(2) After the death of the data subject, processing of his or her personal data is permitted only with the consent of the successors of the data subject, except in the case:
1) 10 years have passed since the death of the data subject;
2) 20 years have passed since the death of a data subject who was a minor;
3) personal data are processed under any other legal bases.

(3) In the case of several successors, processing of the personal data of the data subject is permitted with the consent of any of them.

(4) The consent specified in subsection (1) of this section is not required if the processed personal data only contain the data subject's name, sex, date of birth and death, the fact of death, and the time and place of burial.

§ 10. Processing of personal data in connection with violation of obligation

(1) Transmission of personal data related to violation of any obligation to third parties and processing of the transmitted data by any third party is permitted for the purpose of assessment of the creditworthiness of the data subject or for any other similar purposes and only in the case the controller or processor has verified the accuracy of the data transmitted and the legal basis for transmission of personal data and registered the data transmission.

(2) Collection and transmission of data to third parties for the purposes specified in subsection (1) of this section is not permitted if:
1) special categories of personal data are processed for the purposes of Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council;
2) these are data 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;
3) it would excessively damage the rights or freedoms of the data subject;
4) less than 30 days have passed from the violation of a contract;
5) more than five years have passed from the end of the violation of an obligation.

§ 11. Processing of personal data in public places

Unless otherwise provided by law, upon making in public places of audio or visual recordings intended for future disclosure, the consent of data subjects shall be substituted by an obligation to notify the data subjects thereof in a manner which allows the persons to understand the fact of the recording of the audio or visual images and to give the persons an opportunity to prevent the recording of their person if they so wish. The notification obligation does not apply in the case of public events, recording of which for the purposes of disclosure may be reasonably presumed.

Chapter 4
PROCESSING OF PERSONAL DATA BY LAW ENFORCEMENT AUTHORITIES IN PREVENTION, DETECTION AND PROCEEDINGS OF OFFENCES AND EXECUTION OF PUNISHMENTS

Division 1
General Provisions

§ 12. Application of this Chapter

(1) This Chapter shall apply to processing of personal data by law enforcement authorities in the prevention, detection and proceedings of offences and execution of punishments.

(2) This Chapter shall not apply to processing of personal data upon exercise of state supervision and administrative supervision.

(3) This Chapter prescribes the specifications applicable to law enforcement authorities. Regulation (EU) 2016/679 of the European Parliament and of the Council shall not apply to law enforcement authorities, unless otherwise provided for in this Act.

§ 13. Terms

(1) Terms in this Chapter shall have the meaning specified in Article 4 and Article 9(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council.

(2) For the purposes of this Chapter, law enforcement authorities are deemed to include any agencies or structural entities of agencies which are competent pursuant to law to prevent, detect and proceed offences and execute punishments.

Division 2
Principles

§ 14. Principles of processing personal data

The following principles have to be complied with upon processing of personal data:
1) legality and fairness – personal data are processed legally and fairly;
2) purposefulness – personal data are collected for specified, explicit and legitimate purposes and they shall not be processed in any manner which is incompatible with these purposes;
3) quality – personal data must be adequate and appropriate and must not be excessive given the purposes of the data processing;
4) accuracy – personal data must be accurate and, if necessary, kept up to date; reasonable measures are taken to ensure that any personal data which are inaccurate with respect to the purpose of data processing shall be erased or rectified without delay;
5) retention – personal data are retained in the format which enables to identify the data subject only until this is necessary for achievement of the purpose for which the personal data is processed;
6) security – personal data are processed in a manner that ensures appropriate security thereof, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of implementing appropriate technical or organisational measures.

§ 15. Lawfulness of processing of personal data

Law enforcement authorities may process personal data pursuant to law if the processing thereof is required for performance of the functions arising from the purpose of prevention, detection and proceedings of offences and execution of punishments.

§ 16. Processing of personal data for purposes different from initial ones

(1) Processing of personal data by the same or another controller for other purposes provided for in subsection 12 (1) of this Act, which are not the initial purposes for which the personal data was collected, is permitted insofar as:
1) the controller has the grounds pursuant to law or the legislation of the European Union for processing of personal data for such purposes; and
2) such processing of personal data is required according to law or the legislation of the European Union and it is proportional with the purpose pursued.

(2) Personal data collected or to be collected by law enforcement authorities for the purposes provided for in subsection 12 (1) of this Act may not be processed for any other purposes, except in the cases provided for in subsection (1) of this section or if such processing is permitted by law or the legislation of the European Union. If personal data are processed for such other purposes, Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply, except in the case personal data are processed in the course of such activities which are not in the scope of regulation of the specified regulation. In any situation where the purposes of processing are not in the scope of application of the specified regulation, the Estonian law shall apply.

(3) If law enforcement authorities also perform, in accordance with law, other functions besides those which are performed for the purposes provided for in subsection 12 (1) of this Act, Regulation (EU) 2016/679 of the European Parliament and of the Council shall apply to processing of personal data for such purposes. In any situation where the purposes of processing are not in the scope of application of the specified regulation, the Estonian law shall apply.

§ 17. Retention of personal data

(1) A retention period shall be established for processed personal data by law or regulation. In exceptional cases where no retention period has been established by law or regulation for personal data, the controller must establish this term.

(2) The retention period established pursuant to subsection (1) of this section may be extended only in justified cases, except when the retention period is provided for in a legislative act.

(3) If no specific retention period can be established, the controller must implement legal and technological measures which enable to continuously assess the need for continued processing of the data.

(4) If the term for retention of personal data expires, the controller and processor are required to permanently erase the personal data. For this purpose, the controller must implement appropriate legal and technological measures.

§ 18. Differentiation between different categories of data subjects

If possible and appropriate, the controller shall distinguish, upon processing of personal data, between persons subject to proceedings, suspects, accused, injured parties, witnesses, imprisoned persons, detained persons, probationers and other persons as different categories of data subjects.

§ 19. Distinguishing of personal data based on assessments

The controller shall distinguish, as far as possible, personal data based on facts from personal data based on personal assessments.

§ 20. Specifications for processing of personal data of special categories

(1) Processing of personal data of special categories is permitted only if this is strictly necessary and only in the following cases:
1) admissibility of processing is provided for in the legislation;
2) processing is necessary in order to protect the vital interests of the data subject or of any other natural person; or
3) processing relates to personal data which are manifestly made public by the data subject.

(2) Appropriate safeguards for protection of the rights and freedoms of data subjects apply to processing of personal data of special categories specified in subsection (1) of this section.

§ 21. Automatic processing

(1) It is prohibited to make a decision based on only automatic processing, including profiling, if it brings adverse legal consequences for the data subject pertaining to the data subject or has any other significant effect on the data subject. Such decision may be made if making of the decision is permitted by law which provides for appropriate measures to protect the rights and freedoms and legitimate interests of the data subjects.

(2) The data subject has the right to raise objections to the decision specified in subsection (1) of this section to the controller for the protection of the data subject's legitimate interests.

(3) The decision specified in subsection (1) of this section must not be based on personal data of special categories, except in the case appropriate measures are applied for the protection of the rights, freedoms and legitimate interests of the data subjects.

(4) It is prohibited to make decisions based on profiling as a result of which natural persons are discriminated on the basis of special categories of personal data.

Division 3
Rights of Data Subjects

§ 22. Information to be made available to data subjects

(1) The controller is required to disclose the following information:
1) the intended purpose of processing of personal data;
2) the right of the person to access his or her data and to rectify, erase or restrict thereof and the procedure for the exercise of these rights;
3) the name and contact details of the controller and data protection specialist;
4) the contact details of the Estonian Data Protection Inspectorate;
5) the right to file a complaint to the Estonian Data Protection Inspectorate, if the rights of data subjects have been violated upon processing of personal data.

(2) Disclosure of information on the website of the controller or in any other places which are easily accessible by data subjects is considered to be the disclosure specified in subsection (1) of this section.

§ 23. Information provided upon notification of data subjects

(1) If an obligation to notify data subjects of processing of their personal data is provided by law, the controller shall provide the following additional information to the data subject:
1) the information specified in subsection 22 (1) of this Act;
2) the legal basis for processing of personal data;
3) the retention period of personal data or the bases for determining the retention period;
4) the categories of the recipients to whom transmission of the personal data is permitted;
5) if necessary, any other additional information.

(2) In the cases provided by law, the controller may also transmit the information provided for in subsection (1) of this section to data subjects later, restrict the transmission thereof or not transmit it, if this may:
1) prevent or impair prevention, detection or proceedings of offences or execution of punishments;
2) damage the rights and freedoms of other persons;
3) endanger the national security;
4) endanger protection of public order;
5) hinder formal investigation or proceedings.

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

(1) Data subjects have the right to obtain a confirmation from the processor of processing of their personal data. At the request of the data subject, the processor of personal data shall communicate the following to the data subject:
1) the personal data concerning the data subject and the categories of the personal data concerned;
2) the information available about the origin of the personal data;
3) the purposes of and legal basis for processing of personal data;
4) the recipients or the categories thereof to whom personal data of the data subject have been disclosed;
5) the intended retention period of the personal data or the bases for determining the retention period;
6) the right to apply to the controller for rectification of the personal data of the data subject, erasure or restriction of processing thereof;
7) the right to file a complaint with the Estonian Data Protection Inspectorate and the contact details of the Estonian Data Protection Inspectorate.

(2) In the cases provided by law, the controller may also transmit the information provided for in subsection (1) of this section to data subjects later, restrict the transmission thereof or refuse to issue it if this may:
1) prevent or impair prevention, detection or proceedings of offences or execution of punishments;
2) damage the rights and freedoms of other persons;
3) endanger the national security;
4) endanger protection of public order;
5) hinder formal investigation or proceedings.

(3) The controller shall notify data subjects immediately in writing of restricting access to the information specified in subsection (1) of this section or refusal to access such information and the reasons for it. The controller need not state the reasons if provision of such information would bring about any of the circumstances specified in subsection (2) of this section.

(4) Upon notification of data subjects in accordance with subsection (3) of this section, the controller shall notify the data subjects of their right to address the Estonian Data Protection Inspectorate or a court in order to appeal the decision.

(5) The controller shall document any factual and legal bases of the decision made pursuant to subsection (2) of this section and, if necessary, make this information available to the Estonian Data Protection Inspectorate.

§ 25. Right of data subjects to request rectification and erasure of personal data

(1) Data subjects have the right to demand from the processor rectification of any inaccurate personal data based on facts concerning the data subject.

(2) Data subjects have the right to request from the controller erasure of any incomplete personal data concerning the data subject if this is appropriate in light of the purpose of processing of personal data.

(3) Data subjects have the right to demand from the controller erasure of the personal data collected if:
1) the processing of personal data is not permitted pursuant to law;
2) the principles of processing of personal data were not taken into account upon processing of the personal data; or
3) the controller is obliged to erase the data in order to comply with any obligations under the law, judgment, international agreement or other binging agreements.

(4) The controller shall restrict processing of personal data instead of erasing thereof if:
1) the data subject contests the accuracy of the personal data and the accuracy or inaccuracy thereof cannot be ascertained; or
2) the personal data must be retained for verification purposes.

(5) If the controller has implemented, instead of erasure of personal data, restriction of processing of personal data provided for in clause (4) 1) of this section, the controller must notify the data subject of removal of such restriction.

(6) The controller is required to immediately notify the data subject in writing, if the controller refuses to rectify or erase the personal data or restrict the processing thereof, and state the reasons for the refusal. The controller need not state the reasons if provision of such information would bring about any of the circumstances specified in subsection 24 (2) of this Act.

(7) Upon notification of data subjects in accordance with subsection (6) of this section, the controller shall notify the data subjects of their right to address the Estonian Data Protection Inspectorate or a court in order to appeal the decision.

§ 26. Controller's obligation to notify of rectification, erasure of personal data and restriction of processing thereof

(1) In the case of rectification of personal data, the controller is required to immediately notify a competent authority, from which the incorrect personal data were received, of the rectification and the subject matter of the rectification.

(2) If any personal data have been rectified or erased pursuant to § 25 of this Act or the processing thereof has been restricted, the controller is required to notify the recipients to whom the data had been earlier transmitted.

(3) The recipients specified in subsection (2) of this section are required to rectify or erase the personal data under their responsibility or restrict the processing thereof.

§ 27. Procedure for exercise of rights of data subjects

(1) The controller is required to respond to any applications of data subjects in a concise, intelligible and easily accessible form, using clear and plain wording. If possible, the data subject's request will be answered in the manner requested by the data subject.

(2) The controller shall notify the data subject without any undue delay within one month after the receipt of the application of the activities carried out based on the request of the data subject.

(3) The controller may request the data subject to compensate for any reasonable costs associated with dealing with the request and provided by law or legislation issued pursuant to law or refuse to take the measures requested, if the request of the data subject is unreasonable or excessive.

(4) The controller shall identify the data subject and the right of the data subject to receive information and personal data concerning the data subject or the right to request rectification and erasure of the personal data.

§ 28. Data subject's right to address Estonian Data Protection Inspectorate

(1) If any data subject finds that the rights of the data subject are violated upon processing of personal data, the data subject has the right to address the Estonian Data Protection Inspectorate with a complaint.

(2) The Estonian Data Protection Inspectorate shall notify the data subject of the decision made based on the data subject's complaint and the right to have recourse to courts in order to contest the decision of the Estonian Data Protection Inspectorate.

(3) If a competent supervisory authority of another Member State of the European Union has jurisdiction in solving the complaint of the data subject, the Estonian Data Protection Inspectorate shall refer the data subject to the competent supervisory authority of the other Member State of the European Union for filing the complaint.

Division 4
Obligations of Controllers and Processors

§ 29. Controller and processor of database

(1) The controller shall implement appropriate technical and organisational measures to ensure compliance with the requirements of this Act upon processing of personal data. If necessary, the controller is required to demonstrate compliance with the requirements provided for in this Act.

(2) The controller shall provide the processor with mandatory instructions for processing of personal data and shall be responsible for the processor's compliance with the personal data processing requirements.

(3) The controller may use only such processors which provide sufficient guarantees that they implement appropriate technical and organisational measures in such a manner that processing of personal data will meet the requirements of this Act and ensure the protection of the rights of the data subject.

(4) The processor may involve other processors in processing of personal data only pursuant to law or legislation issued pursuant to law or with a written authorisation of the controller and provided that the powers granted to the processor are not exceeded. In the case of powers granted by a written authorisation, the processor must always notify the controller of adding or replacing of other processors. In this case the controller may state objections to the changes.

(5) If the processor determines the purposes and means for processing of personal data in violation of this Act, the processor in questions shall be the controller with regard to such processing.

§ 30. Designation and obligations of processor

(1) The controller may designate a processor to process personal data pursuant to law, legislation issued pursuant to law or under a written contract which provides for the subject matter and duration of processing of personal data, the nature and purposes thereof, categories of personal data processed and categories of data subjects and the obligations and rights of the controller.

(2) The Act specified in subsection (1) of this section, legislation issued on the basis of the Act or contract shall provide, in particular, that the processor is required to:
1) act only in accordance with the instructions of the controller;
2) ensure that the persons authorised to process personal data would keep the confidentiality of personal data which become known upon performance of their duties;
3) ensure protection of the rights of the data subject;
4) after the end of the provision of data processing services, erase or return to the controller at the choice thereof all the personal data and erase any existing copies thereof, unless otherwise provided by law;
5) make available to the controller any information relating to processing of personal data which is required for demonstrating compliance with the requirements provided for in this section;
6) comply with the terms and conditions provided for in subsection 29 (4) of this Act and this section for involvement of another processors.

§ 31. Joint controllers

(1) Where two or more controllers jointly determine the purposes and means of processing of personal data, they shall be joint controllers.

(2) The responsibility of joint controllers and the scope of the obligations thereof shall be determined in law, legislation issued pursuant to law or a contract entered into between joint controllers.

(3) A contact point through which data subjects are able to exercise their rights shall be determined in the contract specified in subsection (2) of this section for the data subjects.

(4) The data subject may exercise the rights under this Act with respect to each controller.

§ 32. Processing of personal data in name of controller and processor

(1) Any person who processes personal data in the name of a controller or processor is required to process these data only in accordance with the instructions given by the controller, unless otherwise provided by law.

(2) The right of the person to process personal data in the name of the controller or processor must be based on law, legislation issued pursuant to law, contract entered into between the controller or processor and the person or the legal instrument governing the service relationship.

§ 33. Data protection by design and by default

(1) The controller and processor shall take technical and organizational measures upon determining the means of processing and for processing of personal data and implement them consistently.

(2) The controller and processor shall implement appropriate technical and organizational measures which ensure that by default only the personal data are processed which are required for achievement of each specific purpose of processing.

§ 34. Personal data processing requirements

In the processing of personal data, the controllers and processors are required to:
1) rectify inaccurate personal data;
2) erase personal data, if processing of the personal data is not permitted pursuant to law or this does not conform to the principles of processing of personal data;
3) notify the recipient if the personal data have been transmitted illegally or if inaccurate personal data have been transmitted;

4) co-operate with the Estonian Data Protection Inspectorate.

§ 35. Personal data transmission requirements

(1) The controller is required to take and implement appropriate measures in order to avoid transmission or making available of incomplete, inaccurate or outdated personal data.

(2) If possible, the controller shall add, upon transmission of personal data, the required information which allows the competent authority which receives the data to assess the accuracy, integrity, reliability and relevance of the personal data.

(3) If special terms and conditions apply to processing of personal data, the controller shall notify the receiver upon transmission of such personal data of the terms and conditions in questions and the requirement to comply with them.

(4) Upon transmission of personal data to other receivers in the European Union and agencies established in accordance with Chapters 4 and 5 of Section V of the Treaty on the Functioning of the European Union, no special terms and conditions for processing of personal data shall apply compared to those which are applied to transmission of personal data within the country.

§ 36. Logging

(1) The controller and processor must keep logs at least of the following personal data processing activities carried out in automated systems:
1) collection;
2) amendment;
3) reading;
4) disclosure;
5) transmission;
6) combination;
7) erasure.

(2) Logs recording reading, disclosure and transmission must enable to ascertain the reasoning for conduct of the specified activities, the date and time thereof and the information about the person who read, disclosed or transmitted the personal data, and the names of the recipients of such personal data.

(3) It is allowed to use the logs for verification of legality of personal data processing activities, internal monitoring, ensuring integrity and security of personal data and for offence proceedings.

(4) At the request of the Estonian Data Protection Inspectorate, the controller and processor shall make the information specified in subsection (1) of this section available to the Estonian Data Protection Inspectorate.

(5) The controller shall establish the retention periods of logs.

§ 37. Records of personal data processing activities

(1) The controller shall maintain a record of all the types of personal data processing activities under its responsibility. The following information must be recorded:
1) the name and contact details of the controller and, where appropriate, joint controller;
2) the name and contact details of the data protection specialist;
3) the purposes of processing of personal data;
4) the recipients and the categories thereof to whom the personal data have been or will be disclosed;
5) the description of the categories of data subjects and of the categories of personal data;
6) where appropriate, the use of profiling;
7) where appropriate, types of transmission of personal data to third countries or international organizations;
8) information on the legal basis of processing of personal data;
9) if possible, time limits prescribed for erasure of special categories of personal data;
10) if possible, a description of the organizational and technical security measures taken to process personal data pursuant to § 43 of this Act.

(2) The processor shall record all the types of operations related to processing of personal data made in the name of the controller. The following information must be recorded:
1) the name and contact details of the processor, and the name and contact details of the controller in the name of whom the processor operates;
2) where appropriate, the name and contact details of the data protection officer;
3) the types of personal data processing carried out in the name of the controller;
4) where appropriate, transmission of personal data to third countries or international organizations, including data for identification of the third country or international organization in question;

5) if possible, a description of the organizational and technical security measures taken to process personal data pursuant to § 43 of this Act.

(3) The information specified in subsections (1) and (2) of this section shall be recorded in a format which can be reproduced in writing.

(4) At the request of the Estonian Data Protection Inspectorate, the controller or the processor shall make the information specified in subsections (1) and (2) of this section available to the Estonian Data Protection Inspectorate.

§ 38. Data protection impact assessment

(1) The controller shall assess, prior to processing of personal data, the impact of intended personal data processing operations to the protection of personal data, if the processing of personal data may involve a great risk for the personal rights and freedoms of natural persons taking into account the nature, extent, context and purposes of processing.

(2) The impact assessment must include at least the following:
1) a systematic description of the intended personal data processing operations and processing purposes;
2) an assessment of the need and proportionality of personal data processing operations taking into account the purposes of processing of personal data;
3) an assessment of the risks to the rights and freedoms of data subjects;
4) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.

§ 39. Consultation with Estonian Data Protection Inspectorate

(1) If the controller or processor intends to process personal data which are entered into a new filing system to be created, the controller or processor must first consult the Estonian Data Protection Inspectorate in the following cases:
1) the data protection impact assessment issued pursuant to § 38 of this Act indicates that the processing of personal data would result in a high risk in the absence of measures taken by the controller;
2) the nature of processing of personal data involves a high risk to the rights and freedoms of data subjects.

(2) For assessment of conformity with personal data processing requirements, the controller shall submit the following information to the Estonian Data Protection Inspectorate:
1) the data protection impact assessment provided for in § 38 of this Act;
2) the purposes and manner of intended personal data processing;
3) the measures and guarantees prescribed for the protection of the rights and freedoms of data subjects;
4) the contact details of the data protection officer, where applicable;
5) where appropriate, responsibilities of controllers, joint controllers and processors upon processing of personal data;
6) other information requested by the Estonian Data Protection Inspectorate.

(3) If, in the opinion of the Estonian Data Protection Inspectorate, the intended processing of personal data specified in subsection (1) of this section would violate the requirements of this Act, the Estonian Data Protection Inspectorate shall give written advice to the controller and, where appropriate, the processor on how to bring the data processing into compliance with the requirements of this Act.

(4) The Estonian Data Protection Inspectorate shall give advice to the controller or processor within six weeks as of the receipt of the information specified in subsection (2) of this section.

(5) The term specified in subsection (4) of this section may be extended by one month, taking into account the complexity of the intended processing of personal data. The Estonian Data Protection Inspectorate shall notify the controller or processor of extension of the term within one month after receipt of the consultation request. The reasons for extending the term have to be indicated.

(6) The Estonian Data Protection Inspectorate may prepare a list of the personal data processing operations in the case of which the earlier consultations specified in subsection (1) of this section are required.

Division 5
Data Protection Specialist

§ 40. Designation of data protection specialist

(1) Law enforcement authorities designate data protection specialists. Courts are released from this obligation upon performance of the function of administration of justice.

(2) Law enforcement authorities may designate one data protection specialist for several agencies or bodies depending on the structure and size of these organizations.

(3) Designation of a data protection specialist shall be based on his or her professional skills and expert knowledge of data protection legislation and practice and his or her ability to perform the functions provided for in § 41 of this Act.

(4) A data protection specialist may be an official or employee in the service of a law enforcement authority or fulfil the tasks on the basis of a service contract.

§ 41. Tasks of data protection specialist

(1) A data protection specialist shall perform at least the following tasks:
1) inform and advise the law enforcement authority and the officials and employees who process personal data on behalf of the latter in connection with their obligations under this Act and other data protection standards of the European Union or its Member States;;
2) ensure consistency with this Act, if necessary, with data protection standards of the European Union or its Member States and the internal policies of the controller which concern the principles of personal data protection and awareness-raising and training of officials and employees involved in processing of personal data;
3) provide advise as regards the data protection impact assessment and monitor its performance pursuant to § 38 of this Act;
4) co-operate with the Estonian Data Protection Inspectorate;
5) act as the contact person in the issues of personal data processing for the Estonian Data Protection Inspectorate, including in the course of the earlier consultation provided for in § 39 of this Act, and also consult in other issues, if necessary.

(2) The data protection specialist of a court shall not perform the tasks specified in subsection (1) of this section with regard to any activities of the court related to administration of justice.

(3) A data protection specialist may perform other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests for the data protection specialist.

§ 42. Position of data protection specialist

(1) The controller shall ensure that the data protection specialist is involved, properly and in a timely manner, in all the issues which relate to the protection of personal data.

(2) The controller shall support the data protection specialist in performing the tasks referred to in § 41 of this Act by providing the resources necessary to carry out the tasks in question and access to personal data and processing operations thereof, and to maintain his or her expert knowledge.

(3) The provisions of Article 38(3)-(6) of Regulation (EU) No 2016/679 of the European Parliament and of the Council apply to the position of a data protection specialist.

Division 6
Security measures of processing personal data and notification of violations related to personal data

§ 43. Security measures of processing personal data

The controller and the processor are required to take and implement organizational and technical security measures to the protect personal data in order to:
1) prohibit access of unauthorised persons to data processing equipment used for processing of personal data;
2) prevent unauthorized reading, copying, modification and removal of storage media;
3) prevent unauthorised input of personal data and unauthorised inspection, modification or deletion of retained personal data;
4) prevent deletion of data processing systems by unauthorised persons by means of data communication equipment;
5) ensure access by users who hold an authorisation for the use of automated data processing systems only to such personal data which are covered by the access authorisation of the users;
6) ensure an opportunity to verify and establish to which agencies personal data have been or may be transmitted or made available using data communication equipment;
7) ensure an opportunity to verify and establish what personal data have been input into automated data processing systems and when and by whom the data were input;

8) prevent unauthorised reading, copying, modification or deletion of personal data during transmissions of personal data or during transportation of storage media;
9) ensure an opportunity to restore installed data processing systems in the case of interruptions;
10) ensure functioning of data processing systems and notification of any faults in the functions thereof;
11) prevent misrepresentation of personal data as a result of system malfunctions.

§ 44. Notification of Estonian Data Protection Inspectorate of personal data breach

(1) If a personal data breach is likely to entail a high risk to the rights and freedoms of natural persons, the controller shall immediately notify the Estonian Data Protection Inspectorate of the breach, if possible within 72 hours after becoming aware thereof.

(2) The processor shall immediately notify the controller after becoming aware of a personal data breach.

(3) The following information shall be submitted in the notice specified in subsection (1) of this section:
1) the subject matter of the breach, including the nature of the personal data breach, if possible, categories of relevant data subjects and their approximate number, and relevant categories of personal data and their approximate number;
2) the name and contact details of the data protection officer;
3) the description of possible consequences of the personal data breach;
4) measures taken or intended by the controller to resolve personal data breaches, including measures to mitigate any adverse impact of possible consequences of breaches.

(4) If the Estonian Data Protection Inspectorate is notified of a personal data breach after the expiry of 72 hours from becoming aware of it, the reasons thereof shall be stated.

(5) If a personal data breach concerns personal data which have been transmitted by a controller of another Member State of the European Union or to a controller of another Member State of the European Union, the information referred to in subsection (3) of this section shall be transmitted without undue delay to the controller of the Member State in question.

(6) The controller shall document all the personal data breaches specified in subsection (1) of this section, including the circumstances of the breaches, the impact thereof and remedial measures taken.

§ 45. Notification of data subject of personal data breach

(1) When a breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall immediately notify the data subject of the personal data breach.

(2) The notification specified in subsection (1) of this section shall describe, in clear and simple language, the nature of the personal data breach and state at least the information specified in clauses 44 (3) 2)-4) of this Act.

(3) The notification specified in subsection (1) of this section shall not be required if at least one of the following conditions is met:
1) the controller has implemented appropriate technological and organizational safeguards and these safeguards have been applied to the personal data affected by the breach;
2) the controller has taken subsequent measures which exclude realisation of the high risk specified in subsection (1) of this section to the rights and freedoms of the data subject;
3) individual notification of the data subject would lead to disproportionate costs and the public has been notified of the breach.

(4) If the controller has not yet notified the data subject of the personal data breach, the Estonian Data Protection Inspectorate may decide, after assessment of the gravity of the breach, whether the notification of the data subject of the personal data breach is required or any of the cases specified in subsection (3) of this section occurs.

(5) The data subject may be notified of the breach specified in subsection (1) of this section later, to a limited extent, or the notification of the data subject may be withheld, if this may:
1) prevent or impair prevention, detection or proceedings of offences or execution of punishments;
2) damage the rights and freedoms of other persons;
3) endanger the national security;
4) endanger protection of public order;
5) hinder formal investigation or proceedings.

Division 7

Transmission of Personal Data to Third Countries and International Organisations

§ 46. General terms and conditions of transmission of personal data to third countries and international organisations

(1) It is permitted to transmit personal data to third countries or international organisations only in the case all the following terms and conditions are met:
1) transmission is necessary for prevention, detection or processing of offences or execution of punishments;
2) personal data are transmitted to the controller in any third country or international organisation that is competent to prevent, detect and proceed offences or execute punishments;
3) consent of another Member State of the European Union for further use of the data, if the data transmitted have been received from this Member State;
4) the European Commission has adopted a decision pursuant to Article 36 of Directive (EU) 2016/680 of the European Parliament and Council on adequacy of the protection or, in the absence of such decision, the safeguards specified in § 47 of this Act or in the absence thereof the exception specified in § 48 of this Act is applied;
5) it is ensured upon transmission of personal data that the controller that transmits data has given an earlier consent for further transmission of personal data to another third country or international organization.

(2) If the authorisation specified in clause (3) 1) of this section for transmission of personal data cannot be obtained in due time and transmission of personal data is necessary to prevent any immediate and serious threats to the public order of the state or any third country or to protect essential interest of the state, the personal data may be transmitted without the authorisation specified in clause (3) 1) of this section. The competent authority of the Member State of the European Union which transmitted personal data shall be immediately notified of the data exchange provided for in this subsection.

(3) When giving the consent specified subsection clause (1) 5) of this section, the controller or processor shall *inter alia*take into consideration the gravity of the offence, the purpose of initial transmission of personal data and the protection level of personal data in this third country or international organization where the personal data are sent.

(4) If the European Commission has adopted the decision specified in Article 36(5) of Directive (EU) 2016/680 of the European Parliament and of the Council, personal data may be transmitted to third countries or international organizations pursuant to §§ 47 and 48 of this Act.

§ 47. Transmission of personal data subject to application of appropriate safeguards

In the absence of the decision of the European Commission specified in clause 46 (1) 4) of this Act on the adequacy of the protection, personal data may be transmitted to third countries or international organizations in the following cases:
1) the appropriate safeguards taken for the protection of personal data are provided for in a legally binding legal instrument;
2) the controller has assessed all the circumstances relating to transmission of personal data and found that all the safeguards appropriate from the point of view of protection of personal date have been taken.

§ 48. Transmission of personal data in exceptional cases

(1) If the absence of the decision of the European Commission specified in clause 46 (1) 4) of this Act or in the absence of appropriate safeguards specified in § 47 of this Act, transmission of personal data to third countries or international organizations is permitted if this is required in order to:
1) protect the rights and freedoms of data subjects or any other persons;
2) protect the legitimate interests of data subjects;
3) prevent immediate and serious threat to public order;
4) prevent, detect or process offences or execute punishments; or
5) compile, submit or defend a particular legal claim related to the aim of prevention, detection or processing of a particular offence or enforcement of punishment.

(2) If the rights of the data subject outweigh the interest provided for in clauses (1) 4) and 5) of this section, transmission of personal data shall not be permitted.

§ 49. Transmission of personal data to recipients in third countries

Personal data may be transmitted directly to a recipient in any third country if all the following conditions are met::

1) the transmission is strictly necessary for performance of the tasks of the law enforcement authority, which transmits the personal data, for the purpose of prevention, detection and proceeding of offences or execution of punishments;
2) the public interest outweighs the rights and freedoms of the data subject;
3) the transmission of personal data to an agency of any third country, which is competent to prevent, detect and process the offence or execute the punishment, is not effective or appropriate;
4) the agencies of third countries which are competent to prevent, detect and proceed offences or execute punishments shall be notified immediately, except in the case this is not effective or appropriate;;
5) the recipient shall be notified of the specific purpose of processing of personal data and is directed to process personal data only for the specified purpose.

§ 50. Notification of Estonian Data Protection Inspectorate and documentation of transmission of personal data

(1) The controller or processor shall provide an overview to the Estonian Data Protection Inspectorate of transmission of personal data pursuant to clause 47 2) and § 49 of this Act at least once a year.

(2) If personal data is transmitted pursuant to clause 47 2), subsection 48 (1) or § 49 of this Act, the controller or processor shall document such transmission, including the date and time of transmission, the details of the receiving competent authority, the explanation of transmission and the personal data transmitted.

(3) At the request of the Estonian Data Protection Inspectorate, the controller or processor shall make the information specified in subsection (2) of this section available to it.

Chapter 5
STATE AND ADMINISTRATIVE SUPERVISION

Division 1
Supervisory Authority

§ 51. Formation of independent supervisory authority

(1) An independent supervisory authority for the purposes of Article 51(1) of Regulation (EU) 2016/679 of the European Parliament and the Council and Article 41 of Directive (EU) 2016/680 of the European Parliament and the Council is the Estonian Data Protection Inspectorate.

(2) In the performance of its functions, the Estonian Data Protection Inspectorate is independent and acts pursuant to this Act, Regulation (EU) 2016/679 of the European Parliament and the Council, other Acts and legislation established on the basis thereof.

§ 52. Qualifications required to be appointed as head of Estonian Data Protection Inspectorate

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

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

§ 53. Security check of candidate for head of Estonian Data Protection Inspectorate

(1) The candidate for head of Estonian Data Protection Inspectorate must pass a security check before being appointed the head of Estonian Data Protection Inspectorate, except if he or she has a valid access authorisation to access state secrets classified as top secret or, if at the time of becoming a candidate, he or she holds a position which grants the right by virtue of office to access all classifications of state secrets.

(2) The security check of the candidate for the head of Estonian Data Protection Inspectorate shall be carried out 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 the head of Estonian Data Protection Inspectorate shall submit a completed form for an applicant for an authorisation to access state secrets classified as top secret to the Security Police Board through the Ministry of Justice, and 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, communicate the information gathered as a result of the security check to the minister responsible for the area and provide an opinion concerning the compliance of the candidate for the head of

Estonian Data Protection Inspectorate with the conditions for the issue of an authorisation for access to state secrets.

(5) In the cases where the authority of the head of Estonian Data Protection Inspectorate has terminated prematurely, the security check of the candidate for the head of Estonian Data Protection Inspectorate shall be carried out 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 carrying out 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 circumstances specified in clause 3) or 4) may become evident within one month.

(6) Based on the information gathered in the course of the security checks carried out, a candidate for the position of the head of the Estonian 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 Estonian Data Protection Inspectorate may be appointed to office later than the above term after passing a new security check.

§ 54. Appointment to and dismissal from office of head of Estonian Data Protection Inspectorate

(1) The Government of the Republic shall appoint the head of Estonian 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) Before premature dismissal from office of the head of the Estonian Data Protection Inspectorate, the opinion of the Constitutional Committee of the *Riigikogu*shall be heard.

§ 55. Competence of Estonian Data Protection Inspectorate upon accreditation of certification authority

The competent authority for the purposes of Article 43(1) of Regulation (EU) 2016/679 of the European Parliament and the Council, which is competent to accredit certification authorities that have an appropriate level of expertise in relation to data protection is the Estonian Data Protection Inspectorate.

Division 2
Exercise of State and Administrative Supervision

§ 56. Competence of Estonian Data Protection Inspectorate upon exercise of state and administrative supervision

(1) State and the administrative supervision over compliance with the requirements provided for in this Act, legislation established on the basis thereof and Regulation (EU) 2016/679 of the European Parliament and of the Council and the requirements established in other Acts for processing of personal data shall be exercised by the Estonian Data Protection Inspectorate.

(2) In addition to the provision of Article 57 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council, the Estonian Data Protection Inspectorate is competent to:
1) improve the awareness and understanding of the public, controllers and processors of the risks in the processing of personal data, the standards and safeguards in force for processing and the rights related to processing of personal data; the Estonian Data Protection Inspectorate may give recommended instructions for the performance of this function;
2) provide information to data subjects upon request about the exercise of the rights arising from this Act and, where appropriate, co-operate for this purpose with the supervisory authorities of other Member States of the European Union;
3) if necessary, initiate misdemeanour proceedings and impose a punishment, in the case no other administrative measures allow to achieve compliance with the requirements provided by law or Regulation (EU) 2016/679 of the European Parliament and the Council;
4) co-operate with international data protection supervision organisations and other data protection supervision authorities and other competent foreign authorities and persons;
5) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communications technologies;
6) give advice on the personal data processing operations referred to in § 39 of this Act;
7) participate in the European Data Protection Board;
8) apply administrative coercion on the bases, to the extent and pursuant to the procedure prescribed by Acts;
9) present opinions on own initiative or upon request in the issues related to protection of personal data to the *Riigikogu*, the Government of the Republic, the Chancellor of Justice and other agencies and the public;
10) perform other duties arising from Acts.

(3) In addition to the provisions of Article 57 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council, the Estonian Data Protection Inspectorate has the right to:
1) warn controllers and processors that intended processing operations are likely to infringe this Act;
2) demand rectification of personal data;
3) demand erasure of personal data;
4) demand restrictions on processing of personal data;
5) demand termination of processing of personal data, including destruction or forwarding to an archive;
6) where necessary, immediately apply, in order to prevent damage to the rights and freedoms of persons, organisational, physical or information technology security measures to protect 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;
7) implement temporary or permanent restrictions on processing of personal data, including prohibition on processing of personal data;
8) initiate supervision proceedings on the basis of a complaint or on its own initiative.

§ 57. Special state supervision measures

In order to exercise state supervision provided for in this Act, the Estonian Data Protection Inspectorate may apply the specific state supervision measures provided for in §§ 30-32, 44, 49-53 of the Law Enforcement Act on the basis of and pursuant to the procedure provided for in the Law Enforcement Act.

§ 58. Specifications for state supervision

(1) The Estonian Data Protection Inspectorate may implement upon exercise of state supervision the measures provided for in Article 58 of Regulation (EU) No 2016/679 of the European Parliament and of the Council.

(2) The Estonian 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 public electronic communications networks, except for the data relating to the fact of transmission of messages if identification of an end-user related to the identification tokens is impossible in any other manner.

§ 59. Specifications for administrative supervision

(1) When exercising administrative supervision, the Estonian Data Protection Inspectorate may, upon failure to comply with a precept issued subject to Article 83 (7) of Regulation (EU) 2016/679 of the European Parliament and Council and provisions of §§ 751 and 752 of the Government of the Republic Act, address a superior agency, person or body of the recipient of the precept for supervisory control to be organised or for 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 Estonian 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 Estonian Data Protection Inspectorate of the results of relevant proceedings.

(3) If a state agency who is the processor of personal data fails to comply with the precept of the Estonian Data Protection Inspectorate within the term specified therein, the Estonian Data Protection Inspectorate shall file a protest with an administrative court pursuant to procedure provided for in the Code of Administrative Court Procedure.

§ 60. Penalty payment rate

Upon failure to comply with a precept of the Estonian Data Protection Inspectorate, the actual upper limit of the penalty payment applicable pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act is up to 20,000,000 euros, or in the case of undertakings up to 4 per cent of the total global annual turnover of the undertaking for the previous financial year, whichever amount is the higher.

§ 61. Term for review of complaints

(1) The Estonian Data Protection Inspectorate shall settle a complaint within 30 days after the date of filing the complaint with the Estonian Data Protection Inspectorate.

(2) The Estonian Data Protection Inspectorate may extend the term for review of a complaint by up to 60 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.

(3) If co-operation with other relevant supervisory authorities is necessary for settlement of the complaint, review of the complaint shall be extended by a reasonable time period which is necessary to hear the co-operating other supervisory authorities or to state its opinion.

Chapter 6

LIABILITY

§ 62. Violation of obligations of controller and processor

(1) Violation of the obligations of controllers and processors provided for in Articles 8, 11, 25-39, 42 and 43 of Regulation (EU) No 2016/679 of the European Parliament and of the Council
is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 63. Violation of certification procedure

(1) Violation of the certification procedure provided for in Articles 42 and 43 of Regulation (EU) No 2016/679 of the European Parliament and of the Council
is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 64. Violation of procedure for supervision over compliance with code of conduct

(1) Violation of the procedure for supervision over compliance with the code of conduct provided for in Article 41(4) of Regulation (EU) No 2016/679 of the European Parliament and of the Council
is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 65. Violation of personal data processing principles

(1) Violation of the principles of processing personal data provided for in Article 5 of Regulation (EU) 2016/679 of the European Parliament and Council, and violation of the procedure for giving the data subject's consent provided for in Articles 5-7 and 9 of the same Regulation
is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 66. Violation of data subject's rights

(1) Violation of the rights of a data subject provided for in Articles 12-22 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council
is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 67. Violation of procedure for transmission of personal data

(1) Violation of the procedure for transmission of personal data provided for in Articles 44-49 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council
is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 68. Violation of procedure established for specific principles of personal data processing

(1) Violation of the procedure established for specific principles of personal data processing provided for in Chapter 2 of this Act

is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 69. Failure to comply with orders of Estonian Data Protection Inspectorate

(1) Failure to comply with the order provided for in Article 58(2) of Regulation (EU) No 2016/679 of the European Parliament and of the Council
is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 70. Violation of granting access to Estonian Data Protection Inspectorate

(1) Failure to comply with the order issued based on the investigative powers provided for in Article 58(1) of Regulation (EU) 2016/679 of the European Parliament and Council, if the Estonian Data Protection Inspectorate is thereby refused access to personal data, other information or premises,
is punishable by a fine of up to 20,000,000 euros.

(2) The same act, if committed by a legal entity,
is punishable by a fine of up to 20,000,000 euros or up to 4 per cent of its total global annual turnover for the previous financial year, whichever amount is the higher.

§ 71. Illegal processing of personal data outside performance of employment or service duties

Illegal collection, viewing, reading, use of personal data, enabling access thereto or making inquiries or extracts thereof by any person who has access to personal data based on his or her employment or service duties, if this does not involve the necessary elements of an offence provided for in §§ 157 and 157[1] of the Penal Code,
is punishable by a fine of up to 200 fine units.

§ 72. Violation of other personal data processing requirements

Violation of personal data protection requirements, if this does not involve the necessary elements of an offence provided for in §§ 62-71 of this Act and §§ 157 and 157[1] of the Penal Code,
is punishable by a fine of up to 200 fine units.

§ 73. Proceedings

The Estonian Data Protection Inspectorate is the extra-judicial body which conducts proceedings in misdemeanour proceedings provided for in this section.

Chapter 7
IMPLEMENTING PROVISIONS

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

(1) The data of the register of processors of personal data and persons responsible for protection of personal data shall be retained in archived form for the term of up to five years after entry into force of this Act. Upon expiry of the term, the registry data shall be erased.

(2) In order to access the registry data, an application shall be filed with the Estonian Data Protection Inspectorate.

(3) A register entry concerning processing of sensitive personal data is informative until the initial expiry date specified for it.

§ 75. Repeal of Personal Data Protection Act

The Personal Data Protection Act (RT I 2007, 24, 127) is repealed.

§ 76. Entry into force of Act

This Act enters into force on 15 January 2019.

[1]Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 04.05.2016, pp. 89-131).

Eiki Nestor
President of the Riigikogu