Text consolidated by Valsts valodas centrs (State Language Centre) with amending laws of:
24 October 2002 [shall come into force from 27 November 2002];
19 December 2006 [shall come into force from 1 January 2007];
1 March 2007 [shall come into force from 1 September 2007];
21 February 2008 [shall come into force from 6 March 2008];
12 June 2009 [shall come into force from 1 July 2009];
6 May 2010 [shall come into force from 2 June 2010];
21 June 2012 [shall come into force from 18 July 2012];
6 February 2014 [shall come into force from 7 March 2014].
If a whole or part of a section has been amended, the date of the amending law appears in square brackets at the end of the section. If a whole section, paragraph or clause has been deleted, the date of the deletion appears in square brackets beside the deleted section, paragraph or clause.

The *Saeima*[1] has adopted and
the President has proclaimed the following law:

Personal Data Protection Law

Chapter I
General Provisions

Section 1.

The purpose of this Law is to protect the fundamental human rights and freedoms of natural persons, in particular the inviolability of private life, with respect to the processing of data regarding natural persons (hereinafter – personal data).

Section 2.

The following terms are used in this Law:

1) **data subject** – a natural person who may be directly or indirectly identified;

2) **consent of a data subject** – a freely, unmistakably expressed affirmation of the wishes of a data subject, by which the data subject allows his or her personal data to be processed in conformity with information provided by the administrator in accordance with Section 8 of this Law;

3) **personal data** – any information related to an identified or identifiable natural person;

4) **personal data processing** – any operations carried out regarding personal data, including data collection, registration, recording, storing, arrangement, transformation, using, transfer, transmission and dissemination, blockage or erasure;

5) **personal data processing system** – a structured body of personal data recorded in any form that is accessible on the basis of relevant person identifying criteria;

6) **personal data processor** – a person authorised by an administrator, who carries out personal data processing upon the instructions of the administrator;

7) **recipient of personal data** – a natural or a legal person to whom personal data are disclosed;

8) **sensitive personal data** - personal data which indicate the race, ethnic origin, religious, philosophical or political convictions, or trade union membership of a person, or

[1] The Parliament of the Republic of Latvia

provide information as to the health or sexual life of a person;

9) **administrator** – a natural person or a legal person, State or local government institution who itself or together with others determines the purposes and the means of processing of a personal data processing, as well as is responsible for a personal data processing in accordance with this Law;

10) **third person** – any natural person or legal person, except for a data subject, an administrator, a personal data processor and persons who have been directly authorised by an administrator or a personal data processor;

11) **personal identification code** – a number that is granted for the identification of a data subject.

[24 October 2002; 1 March 2007; 6 February 2014]

Section 3.

(1) This Law, taking into account the exceptions specified in this Law, applies to the processing of all types of personal data, and to any natural person or legal person if:

1) the administrator is registered in the Republic of Latvia;

2) data processing is performed outside the borders of the Republic of Latvia in territories, which belong to the Republic of Latvia in accordance with international agreements;

3) in the territory of the Republic of Latvia is located equipment, which is used for the processing of personal data, except for the cases when the equipment is used only for the transferring of personal data via the territory of the Republic of Latvia.

(2) In the cases referred to in Paragraph one, Clause 3 of this Section, the administrator shall appoint an authorised person who is a registered legal person in the Republic of Latvia or a Latvian citizen, a Latvian non-citizen or foreign national for whom a permanent residence permit has been issued and an address of the place of residence is declared in Latvia. The administrator prior to the commencement of data processing shall inform in writing the Data State Inspectorate regarding the appointed authorised person. The appointment of the authorised person shall not release the administrator from the responsibility for compliance with this Law.

(3) This Law shall not apply to the processing of personal data which natural persons perform for personal or household and family purposes, moreover the personal data are not disclosed to third persons.

(4) If there are several administrators of the processing of personal data and obligations of each administrator are not provided for in the laws and regulations, they have the right to agree in writing regarding mutual obligations to comply with this Law.

[24 October 2002; 1 March 2007; 6 February 2014]

Section 4.

This Law, taking into account the exceptions, which are specified in the Law On Official Secrets, shall regulate the protection of personal data, which have been declared to be official secret objects.

[24 October 2002]

Section 5.

(1) Sections 7, 8, 9, 11 and 21 of this Law shall not apply if personal data are processed for journalistic purposes in accordance with the Law on the Press and Other Mass Media, artistic or literary purposes, and it is not prescribed otherwise by law.

(2) The provisions of Paragraph one of this Section shall be applied taking into account the rights of persons to inviolability of private life and freedom of expression.
[1 March 2007; 6 February 2014]

Chapter II
General Principles for Processing of Personal Data

Section 6.

Every natural person has the right to protection of his or her personal data.

Section 7.

Processing of personal data is permitted only if not prescribed otherwise by law, and if at least one of the following conditions exists:

1) the data subject has given his or her consent;

2) the processing of data results from contractual obligations of the data subject or, taking into account a request from the data subject, the processing of data is necessary in order to enter into the relevant contract;

3) the processing of data is necessary to an administrator for the performance of his or her duties as specified by law;

4) the processing of data is necessary to protect vitally important interests of the data subject, including life and health;

5) the processing of data is necessary in order to ensure that the public interest is complied with, or to exercise functions of public authority for whose performance the personal data have been transferred to an administrator or transmitted to a third person;

6) the processing of data is necessary in order to, complying with the fundamental human rights and freedoms of the data subject, exercise lawful interests of the administrator or of such third person as the personal data have been disclosed to.

[24 October 2002; 1 March 2007]

Section 8.

(1) When collecting personal data from a data subject, an administrator has a duty to provide a data subject with the following information unless it is already available to the data subject:

1) the designation, or given name and surname, as well as address of the administrator;

2) the intended purpose for the personal data processing.

(2) On the basis of a request from the data subject, the administrator has a duty to provide the following information:

1) the possible recipients of the personal data;

2) the right of the data subject to gain access to his or her personal data and of making corrections in such data;

3) whether providing an answer is mandatory or voluntary, as well as the possible consequences of failing to provide an answer;

4) the legal basis for the processing of personal data.

(3) Paragraph one of this Section is not applicable if the conducting of the processing of personal data without disclosing its purpose is authorised by law.

[24 October 2002; 1 March 2007; 6 February 2014]

Section 9.

(1) If personal data have not been obtained from the data subject, an administrator has a duty, when collecting or disclosing such personal data to third persons for the first time, to provide the data subject with the following information:

1) the designation, or given name and surname, and address of the administrator;

2) the intended purpose for the processing of personal data.

(2) [6 February 2014]

(3) Paragraph one of this Section is not applicable, if:

1) the law provides for the processing of personal data;

2) when processing personal data for scientific, historical or statistical researches, for the establishment of the national documentary heritage or provision of official publication, the informing of the data subject requires inordinate effort or is impossible.

[24 October 2002; 1 March 2007; 21 June 2012; 6 February 2014]

Section 10.

(1) In order to protect the interests of a data subject, an administrator shall ensure that:

1) the processing of personal data takes place with integrity and lawfully;

2) the personal data is processed only in conformity with the intended purpose and to the extent required therefor;

3) the personal data are stored so that the data subject is identifiable during a relevant period of time, which does not exceed the time period prescribed for the intended purpose of the data processing;

4) the personal data are accurate and that they are updated, rectified or erased in a timely manner if such personal data are incomplete or inaccurate in accordance with the purpose of the personal data processing.

(2) Personal data processing for purposes other than those originally intended is permissible if it does not violate the rights of the data subject and is carried out for the needs of scientific or statistical research only in accordance with the conditions referred to in Section 9 and Section 10, Paragraph one of this Law.

(3) Paragraph one, Clauses 3 and 4 of this Section are not applicable to the processing of personal data for the establishment of the national documentary heritage or provision of official publication according to the procedures laid down in laws and regulations.

(3^1) A publisher of the official publication shall delete personal data published in the official publication on the basis of the decision of the Data State Inspectorate. The decision of the Data State Inspectorate regarding deletion of personal data published in the official publication may be taken, if violation of the right of a data subject to private life is greater than the benefit of the public from invariability of the official publication.

(4) Personal data processing for the purposes other than those originally intended is permissible in the field of criminal law:

1) to prevent, detect, investigate criminal offence and carry out criminal prosecution or enforce criminal penalty;

2) to use personal data in legal proceeding of an administrative or civil matter, as well as in the activity of officials of State institutions authorised by a law, if it is related to prevention, detection, investigation or criminal prosecution of criminal offences, or enforcement of criminal penalties;

3) to prevent immediate significant threat to public security;

4) if a data subject has given a consent to data processing.

[24 October 2002; 1 March 2007; 6 May 2010; 21 June 2012; 6 February 2014]

Section 11.

The processing of sensitive personal data is prohibited, except in cases where:

1) the data subject has given his or her written consent for the processing of his or her sensitive data;

2) special processing of personal data, without requesting the consent of the data subject, is provided for in the laws and regulations, which regulate employment legal relations, and such laws and regulations guarantee the protection of personal data;

3) processing of personal data is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent;

4) processing of personal data is necessary to achieve the lawful, non-commercial objectives of public organisations and their associations, if such processing of data is only related to the members of these organisations or their associations and the personal data are not transferred to third persons;

5) processing of personal data is necessary for the purposes of medical treatment, the provision of health care services or the administration thereof and the distribution of medicinal products and medical devices or administration thereof;

6) the processing concerns such personal data as necessary for the protection of rights or lawful interests of natural or legal persons in court proceedings;

7) processing of personal data is necessary for the provision of social assistance and it is performed by the provider of social assistance services;

8) processing of personal data is necessary for the establishment of the national documentary heritage and it is performed by the Latvian national archives and accredited private archives;

9) processing of personal data is necessary for statistical research, which is performed by the Central Statistics Bureau;

10) the processing relates to such personal data, which the data subject has him or herself made public;

11) processing of personal data is necessary when performing State administration functions or establishing State information systems laid down in the law;

12) processing of personal data is necessary for the protection of a natural person's or legal person's rights or lawful interests when claiming for indemnity in accordance with the insurance contract;

13) patient's data recorded in medical documents are used in a research in conformity to the Law On the Rights of Patients.

[24 October 2002; 1 March 2007; 21 February 2008; 6 May 2010; 21 June 2012]

Section 12.

Personal data, which relate to the criminal offences, convictions in criminal matters and administrative violations matters, as well as to court adjudication or court file materials, may be processed only by persons laid down in the law and in the cases laid down in the law.

[1 March 2007]

Section 13.

(1) An administrator is obliged to disclose personal data in cases provided for by law to officials of State and local government institutions. The administrator shall disclose the personal data only to such officials of the State and local government institutions as he or she has identified prior to the disclosure of such data.

(2) Personal data may be disclosed on the basis of a written application or agreement, stating the purpose for using the data, if not prescribed otherwise by law. The application for personal data shall set out information as will allow identification of the applicant for the data and the data subject, as well as the amount of the personal data requested.
(3) The personal data received may be used only for the purposes for which they are intended.
[1 March 2007]

Section 13.[1]

Personal identification codes may be processed in one of the following cases:
1) the consent of the data subject has been received;
2) the processing of the identification codes arises from the purpose of the processing of personal data;
3) the processing of the identification codes is necessary to ensure the continuing anonymity of the data subject;
4) a written permit has been received from the Data State Inspectorate.
[1 March 2007]

Section 14.

(1) An administrator may entrust processing of personal data to a personal data processor provided a written contract is entered into between them.
(2) A personal data processor may process personal data entrusted to him or her only within the amount determined in the contract and in conformity with the purposes provided for therein and in accordance with the instructions of the administrator if they are not in conflict with laws and regulations.
(3) Prior to commencing processing of personal data, a personal data processor shall perform safety measures determined by the administrator for the protection of the system in accordance with the requirements of this Law.
[24 October 2002; 1 March 2007]

Chapter III
Rights and Obligations of a Data Subject
[6 February 2014]

Section 15.

(1) In addition to the rights referred to in Sections 8 and 9 of this Law, a data subject has the right to obtain all information that has been collected concerning himself or herself in any personal data processing system.
(2) A data subject has the right to obtain information concerning those natural or legal persons who within a prescribed time period have received information from an administrator concerning this data subject. In the information to be provided to the data subject, it is prohibited to include State institutions, which administer criminal procedures, investigatory operations authorities or other institutions concerning which the disclosure of such information is prohibited by law.
(3) A data subject also has the right to request the following information:
1) the designation, or name and surname, and address of the administrator;
2) the purpose, legal basis and method of the processing of personal data ;
3) the date when the personal data concerning the data subject were last rectified, data extinguished or blocked;
4) the source from which the personal data were obtained unless the disclosure of such

information is prohibited by law;

5) the processing methods used for the automated processing systems, concerning the application of which individual automated decisions are taken;

6) the possibility to use the right referred to in Paragraphs one and two of this Section and Section 16, Paragraph one of this Law.

(3^1) If a data subject requests information in relation to video surveillance, the data subject has a duty to provide the information upon the relevant request of the administrator, which is necessary for the identification of the data subject and requested personal data.

(4) A data subject has the right, within one month from the date of submission of the relevant request (not more frequently than two times a year), to receive free of charge the information referred to in this Section in writing or a justified refusal in writing to provide fully or partly the information referred to in this Section. The provision of information may be refused if a data subject refuses to perform the obligation laid down in Paragraph $3.^1$ of this Section.

(5) A data subject has not the right to receive the information referred to in Paragraphs one, two and three of this Section, if it is prohibited to disclose such information in accordance with the law in the field of national security, State protection, public security, criminal law, as well as with a view to ensure the State financial interests in the tax affairs or supervision of participants of the financial market and macroeconomic analysis.

[24 October 2002; 1 March 2007; 21 February 2008; 21 June 2012; 6 February 2014]

Section 16.

(1) A data subject has the right to request that his or her personal data be supplemented or corrected, as well as that their processing be discontinued or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully processed or are no longer necessary for the purposes for which they were collected. If the data subject is able to substantiate that the personal data are incomplete, outdated, false, unlawfully processed or no longer necessary for the purposes for which they were collected, the administrator has an obligation to rectify this inaccuracy or violation without delay and notify third persons who have previously received the processed data of such.

(2) [1 March 2007]

(3) A data subject has the right to receive a justified reply of an administrator in writing regarding examination of the request within a month from the day of submission of the relevant request.

[1 March 2007; 12 June 2009]

Section 17.

(1) Sections 15 and 16 of this Law are not applicable if the processed data are used only for the needs of scientific and statistical research or the establishment of the national documentary heritage in accordance with laws and regulations and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject.(2) Section 15, Paragraph two and Section 16 of this Law shall not be applied, if a processing of personal data is carried out in accordance with the laws and regulations for the ensuring of an official publication.

[24 October 2002; 21 June 2012; 6 February 2014]

Section 18.

(1) If a data subject disputes an individual decision, which has been taken only upon the basis of automated processed data, and creates, amends, determines or terminates legal relations, the administrator has a duty to review the decision. The administrator may refuse to review such

decision if it has been taken in accordance with law or a contract entered into with the data subject.
(2) A data subject has the right to receive a justified reply of an administrator in writing regarding examination of the request within a month from the day when the request regarding review of the decision is submitted.
[24 October 2002; 1 March 2007; 6 February 2014]

Section 19.

(1) A data subject has the right to prohibit the processing of his or her personal data for commercial purposes, in the cases referred to in Section 7, Clause 6 of this Law, for use in information society services, market and public opinion researches, genealogical researches, except for the cases when it is otherwise provided for in the laws.
(2) A data subject has the right to receive a justified reply of an administrator in writing regarding examination of the request within a month from the day when the request regarding prohibition of the processing of personal data is submitted.
[1 March 2007; 6 February 2014]

Section 20.

If an administrator fails to comply with the obligations laid down in this Law, a data subject has the right to appeal to the Data State Inspectorate the refusal of an administrator to provide the information referred to in Section 15 of this Law or perform the activities referred to in Sections 16, 18 and 19 of this Law, appending the documents attesting that the administrator refuses to comply with or fails to comply with the obligations laid down in the Law.
[12 June 2009; 6 February 2014]

Chapter III[1]
Rights of a Data Subject in Relation to Data Processing in the Eurojust and European Police Office
[21 June 2012]

Section 20.[1]

A data subject has the right to submit a request to the Data State Inspectorate regarding processing of his or her personal data or examination of processing of his or her personal data in the Eurojust or European Police Office.

Section 20.[2]

The Data State Inspectorate upon receipt of the request referred to in Section 20.[1] of this Law shall immediately, however not later than within a month from the day of receipt thereof, resend the request to the Eurojust or European Police Office accordingly for examination and inform a data subject thereon.

Chapter IV
Registration and Protection of Processing of Personal Data
[1 March 2007]

Section 21.

Prior to commencement of the processing of personal data an administrator shall register the processing of personal data with the Data State Inspectorate or assign a natural person – data protection specialist – if the administrator:

1) intends to transfer personal data to a state other than a Member State of the European Union or European Economic Area;

2) intends to process personal data when providing financial or insurance services, carrying out raffles or lotteries, market or public opinion researches, personnel selection or personnel assessment as the form of commercial activity, when providing debt recovery services and credit information processing services as the form of commercial activity;

3) carries out processing of sensitive personal data, except for the cases when the referred-to data processing is carried out for the purposes of accounting, personnel registration (employment legal relations) or if it is done by religious organisations;

4) processes personal data in relation to the criminal offences, criminal records and penalties in administrative violations matters;

5) carries out video surveillance retaining personal data;

6) carries out processing of genetic data.

[6 February 2014]

Section 21.[1]

(1) An administrator has the right not to register personal data processing, if he or she assigns a for personal data protection specialist. A personal data protection specialist is not a personal data processor.

(2) A natural person having acquired a higher education in the field of law, information technologies or similar and who has been trained in accordance with the procedures laid down by the Cabinet shall be assigned as a personal data protection specialist.

(3) An administrator shall grant the necessary means to a personal data protection specialist, ensure him or her with the necessary information and intend the time within the framework of working hours in order for him or her also to perform the duties of the data protection specialist.

(4) An administrator shall register a personal data protection specialist with the Data State Inspectorate.

(5) A register of personal data protection specialists shall be publicly accessible. The following information shall be provided regarding a personal data protection specialists in the register:

1) a person's given name, surname, contact information (address, phone number, electronic mail address);

2) a time period for which a person is assigned;

3) the place of processing of a personal data and information regarding the possibilities to receive the information referred to in Section 22, Paragraph one of this Law.

(6) The Data State Inspectorate shall postpone registration of a personal data protection specialist, if all information referred to in Paragraph five of this Section is not provided.

(7) The Data State Inspectorate shall not register a personal data protection specialist, if:

1) he or she does not comply with the requirements stipulated in this Law;

2) any of the cases referred to in Section 22, Paragraph six of this Law has set in.

(8) The Data State Inspectorate shall exclude a personal data protection specialist from the register in the following cases, if:

1) a submission of the administrator is received regarding exclusion from the register of personal data processing;

2) within a month after registration of a personal data protection specialist an administrator has not lodged a submission regarding exclusion of a personal data processing from the register of personal data processing.

(9) The Data State Inspectorate shall take a decision to register a personal data protection specialist within 15 days following the lodging of the information referred to in Paragraph five of this Section to the Data State Inspectorate.

(10) The Data State Inspectorate may exclude a personal data protection specialist from the register and request the registration of a personal data processing in accordance with Section 22 of this Law, if the Data State Inspectorate determines infringements of this Law in the processing of personal data under the supervision of the personal data protection specialist.

[1 March 2007; 12 June 2009]

Section 21.[2]

(1) A personal data protection specialist shall organise, control and supervise the conformity of the processing of personal data performed by the administrator to the requirements of the Law.

(2) A personal data protection specialist shall establish a register in which the information referred to in Section 22, Paragraph one of this Law shall be included (except for the information referred to in Paragraph one, Clauses 10 and 11 of the same Section) what is provided free-of-charge to a data subject or to the Data State Inspectorate upon their request.

(3) A personal data protection specialist has an obligation to store and not to disclose personal data without a legal justification even after termination of employment, service or other legal relations.

(4) A personal data protection specialist shall draw up an annual account each year regarding his or her activity and submit it to the administrator.

[1 March 2007; 12 June 2009; 6 February 2014]

Section 22.

(1) The institutions and persons referred to in Section 21 of this Law which wish to commence processing personal data shall lodge a submission for registration to the Data State Inspectorate which includes the following information:

1) the name, surname, personal identity number (for a legal person – firm name and registration number), address and telephone number of the administrator;

2) the name, surname, personal identity number (for a legal person – firm name and registration number), address and telephone number of a personal data processor (if any);

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

4) the type of personal data and the purposes of processing of personal data;

5) the categories of data subjects;

6) the categories of recipients of personal data;

7) the intended method of processing of personal data;

8) the planned method of obtaining personal data;

9) the place of processing of personal data;

10) the holder of information resources or technical resources, as well as a person responsible for the security of the information system;

11) technical and organisational measures ensuring the personal data protection;

12) what personal data will be transferred to other states other than Member States of the European Union or the European Economic Area.

(2) The Data State Inspectorate shall identify the processing personal data where risks are possible for the rights and freedoms of data subjects. Pre-registration checking must be determined for such processing of personal data.

(3) When registering a processing of personal data, the Data State Inspectorate shall issue a decision regarding registration of the data processing to an administrator or to a person authorised by him or her. The Data State Inspectorate shall issue a certificate of registration of the processing of personal data for a charge in accordance with a pricelist of paid services approved by the Cabinet upon a request of those persons referred to in Section 21 of this Law who wish to commence processing of personal data.

(4) Prior to changes being made in a processing of personal data, such changes shall be registered in the Data State Inspectorate, except for the information referred to in Paragraph one, Clause 11 of this Section.

(5) If technical and organisational measures of the processing of personal data change so that they significantly impact on the protection of processing of personal data, information thereon shall be submitted within one year to the Data State Inspectorate.

(6) If an administrator changes or operation of the administrator is terminated, he or she shall lodge a submission to the Data State Inspectorate regarding exclusion of a processing of personal data from the register for processing of personal data.

(7) The Data State Inspectorate shall take a decision to exclude an administrator from the register for processing of personal data, if:

1) an administrator has not rectified infringements within the time period indicated by the Data State Inspectorate;

2) an administrator within a month following the making of changes in the processing of personal data has not lodged a submission regarding making of changes in the processing of personal data or has not lodged a submission referred to in Paragraph six of this Section.

(8) The Cabinet shall determine sample forms for the following submissions:

1) a submission for registration of processing of personal data;

2) a submission regarding making of changes in the processing of personal data;

3) a submission for registration of personal data protection specialist;

4) a submission regarding exclusion of the processing of personal data from the register for the processing of personal data;

5) a submission for exclusion of a personal data protection specialist from the register of the Data State Inspectorate.

(9) For the registration of each processing of personal data or the registration of the changes referred to in Paragraph four of this Section, a State fee shall be paid according to the procedures and in the amount laid down by the Cabinet.

[1 March 2007; 6 February 2014]

Section 23.

(1) The Data State Inspectorate shall postpone registration of a processing of personal data or taking of a decision to make changes in the processing of personal data, if:

1) deficiencies have been determined in a submission for the registration of processing of personal data;

2) all of the information referred to in Section 22, Paragraph one of this Law is not provided;

3) a State fee has not been paid;

4) a pre-registration checking is determined for a processing of personal data in accordance with Section 22, Paragraph two of this Law.

(2) The Data State Inspectorate shall not register processing of personal data or take a decision to refuse to make changes in the processing of personal data if:

1) the deficiencies detected and notified by the Data State Inspectorate are not rectified within 30 days;

2) a submission for registration of processing of personal data or a submission regarding making of changes in the processing of personal data has been submitted by a person who is not considered as an administrator within the meaning of his Law;

3) when inspecting the processing of personal data, infringements of the laws and regulations have been determined in the field of personal data protection.

(3) When submitting documents repeatedly after the time period laid down in this Law for rectification of the deficiencies detected, a State fee provided for in this Law shall be paid repeatedly.

(4) In the cases referred to in Paragraph two, Clause 2 of this Section a State fee shall be refunded in accordance with the decision of the Data State Inspectorate.

[1 March 2007; 6 February 2014]

Section 24.

(1) The Data State Inspectorate shall include the information referred to in Section 22, Paragraphs one and four of this Law in the register for processing of personal data, except the information referred to in Paragraph one, Clauses 10 and 11 of the same Section. The register shall be publicly accessible.

(2) Information regarding the registered processing of personal data which is governed by the Law On Official Secrets and the Investigatory Operations Law shall not be included in the register referred to in Paragraph one of this Section.

[1 March 2007]

Section 24.[1]

The registers referred to in Section 21.[1], Paragraph five and Section 24, Paragraph one of this Law shall be a component of the supervisory information system of the processing of personal data. The supervisory information system of the processing of personal data is a State information system, the operation of which is organised and managed by the Data State Inspectorate.

[1 March 2007]

Section 25.

(1) An administrator and personal data processor have a duty to use the necessary technical and organisational measures in order to protect personal data and to prevent their illegal processing.

(2) An administrator shall control the form of personal data entered and the time of recording and is responsible for the actions of persons who carry out processing of personal data.

[24 October 2002; 1 March 2007]

Section 26.

(1) The mandatory technical and organisational requirements for the protection of processing of personal data shall be determined by the Cabinet.

(2) State and local government institutions and private persons, to whom administrative tasks have been delegated, shall draw up a conformity assessment of a processing of personal data,

including also a risk analysis therein, and a report regarding measures performed in the field of information security.
(2^1) Conditions for a conformity assessment of a processing of personal data, procedures for drawing up and submission thereof, as well as a time period shall be determined by the Cabinet.
(3) [12 June 2009]
(4) [12 June 2009]
[24 October 2002; 19 December 2006; 1 March 2007; 12 June 2009; 6 February 2014]

Section 27.

(1) Natural persons involved in processing of personal data shall make a commitment in writing to preserve and not, in an unlawful manner, disclose personal data. Such persons have a duty not to disclose the personal data even after termination of legal employment or other contractually specified relations.
(2) An administrator is obliged to record the persons referred to in Paragraph one of this Section.
(3) When processing personal data, a processor of the personal data shall comply with the instructions of the administrator.
[1 March 2007]

Section 28.

(1) Personal data may be transferred to another state, other than a Member State of the European Union or European Economic Area, or an international organisation, if that state or international organisation ensures such level of data protection as corresponds to the relevant level of the data protection in effect in Latvia.
(2) Exemption from compliance with the requirements referred to in Paragraph one of this Section is permissible if the administrator undertakes to perform supervision regarding the performance of the relevant protection measures or at least one of the following conditions is complied with:

1) the consent of the data subject for transfer of personal data;

2) the transfer of the data is necessary in order to fulfil an agreement between the data subject and the administrator, the personal data are required to be transferred in accordance with contractual obligations binding upon the data subject or also, taking into account a request from the data subject, the transfer of data is necessary in order to enter into a contract;

3) the transfer of the data is required and requested, pursuant to prescribed procedures, in accordance with significant state or public interests, or is required for judicial proceedings;

4) the transfer of the data is necessary to protect the life and health of the data subject;

5) the transfer of the data concerns such personal data as are public or have been accumulated in a publicly accessible register.

(3) The evaluation of the level of personal data protection in accordance with Paragraph one of this Section shall be performed by the Data State Inspectorate and it shall issue permission in writing for the transfer of the personal data.
(4) In order an administrator could supervise the performance of the relevant protection measures, the administrator and recipient of personal data shall enter into a contract regarding transfer of the data. Conditions that are to be included mandatory in the contract regarding transfer of the personal data shall be determined by the Cabinet.
(4^1) Exemptions from compliance with the requirements referred to in Paragraph four of this Section is permissible if:

1) the administrator ensures that binding regulations of the company, containing

principles for processing and protection of personal data, ensure the rights of data subjects and are approved in one of personal data protection supervision institutions of the Member States of the European Union;

2) the administrator enters into the contract in conformity with standard clauses of the contract regarding sending of personal data to third countries approved by the European Commission.

(4^2) Exemptions referred to in Paragraph $4.^1$ of this Section shall not apply to the field of international co-operation, national security and criminal law, and a contract regarding transfer of data shall not be entered into in the referred-to fields.

(5) Personal data may be transferred to other Member State of the European Union or European Economic Area, if that state ensures such level of data protection as corresponds to the relevant level of the data protection in effect in Latvia.

(6) When transferring personal data to other country or international organisation, the relevant restrictions intended for the processing of personal data shall be notified unless they are included in the contract referred to in Paragraph four of this Section.

[24 October 2002; 1 March 2007; 6 May 2010; 6 February 2014]

Section 29.

(1) The supervision of protection of personal data shall be carried out by the Data State Inspectorate, which is subject to the supervision of the Ministry of Justice and operates independently and permanently fulfilling the functions specified in laws and regulations, takes decisions and issues administrative acts in accordance with the law. The Data State Inspectorate is a State administration institution the functions, rights and duties of which are determined by law. The Data State Inspectorate shall be managed by a director who shall be appointed and released from his or her position by the Cabinet pursuant to the recommendation of the Minister for Justice.

(2) The Data State Inspectorate shall act in accordance with by-laws approved by the Cabinet. Every year the Data State Inspectorate shall submit a report on its activities to the Cabinet and shall publish it in the newspaper *Latvijas Vēstnesis* [the official Gazette of the Government of Latvia].

(3) The duties of the Data State Inspectorate in the field of personal data protection are as follows:

1) to supervise compliance of processing of personal data with the requirements of this Law;

2) to take decisions and review complaints regarding the protection of personal data;

3) to register processing of personal data;

4) to propose and carry out activities, as well as take decisions, aimed at raising the effectiveness of personal data protection;

5) [21 June 2012];

6) [12 June 2009]

(4) In the field of personal data protection, the rights of the Data State Inspectorate are as follows:

1) in accordance with the procedures prescribed by laws and regulations, to receive, free of charge, information from natural persons and legal persons as is necessary for the performance of functions pertaining to inspection;

2) to perform inspection of a processing of personal data;

3) to require that data be blocked, that incorrect or unlawfully obtained data be erased or destroyed, or to order a permanent or temporary prohibition of data processing;

4) to bring an action in court for violations of this Law;

5) to cancel a registration certificate of the processing of personal data if in inspecting

the processing of personal data infringements are determined;

6) to impose administrative penalties according to the procedures specified by law regarding infringements of processing of personal data;

7) to perform inspections in order to determine the conformity of processing of personal data to the requirements of laws and regulations in cases where the administrator has been prohibited by law to provide information to a data subject and a relevant submission has been received from the data subject;

8) to perform processing of personal data, including sensitive personal data, necessary for the implementation of the tasks of the Data State Inspectorate.

[24 October 2002; 1 March 2007; 12 June 2009; 21 June 2012; 6 February 2014]

Section 30.

(1) In order to perform the duties referred to in Section 29, Paragraph three of this Law, the director of the Data State Inspectorate and the Data State Inspectorate employees authorised by the director, have the right:

1) to freely enter any non-residential premises where processing of personal data is located, and in the presence of a representative of the administrator carry out necessary inspections or other measures in order to determine the compliance of the procedure of processing of personal data with law;

2) to require written or verbal explanations from any natural or legal person involved in processing of personal data;

3) to require that documents are presented and other information is provided which relate to the processing of personal data being inspected;

4) to require inspection of a processing of personal data, or of any facility or information carrier of such, and to determine that an expert examination be conducted regarding questions subject to investigation;

5) to request assistance of officials of law enforcement institutions or other specialists, if required, in order to ensure performance of its duties;

6) to prepare and submit materials to law enforcement institutions in order for offenders to be held to liability, if required;

7) to draw up an administrative violation report in processing of personal data.

(2) The officials of the Data State Inspectorate involved in registration and inspections shall ensure that the information obtained in the process of registration and inspections is not disclosed, except information accessible to the general public. Such prohibition shall also remain in effect after the officials have ceased to fulfil their official functions.

[24 October 2002; 1 March 2007]

Section 30.[1]

(1) The Data State Inspectorate is a national supervision institution, which carries out the supervision of the national part of the Schengen Information System and verifies whether the rights of a data subject are not infringed in the processing of personal data included in the Schengen Information System.

(2) The Data State Inspectorate shall supervise that in the processing of personal data, which is carried out in co-operation with the European Police Office, the conditions of the processing of personal data laid down in the laws and regulations are complied with.

[1 March 2007; 6 May 2010]

Section 31.

(1) An administrative act issued by an official of the Data State Inspectorate or actual action thereof may be contested to the director of the Data State Inspectorate. The administrative act issued by the director or actual action thereof, as well as a decision regarding the contested administrative act or actual action may be appealed to a court in accordance with the procedures laid down in the law.
(2) A decisions of the director or other official of the Data State Inspectorate regarding blocking of data, contesting and appealing of permanent or temporary prohibition of the data processing shall not suspend the operation of such decision, except the case when it is suspended by a decision of a person examining the submission or application.
[6 May 2010]

Section 32.

If, in infringing this Law, harm or losses have been caused to a person, he or she has the right to receive commensurate compensation.

Transitional provisions

1. Chapter IV of this Law, "Registration and Protection of a Personal Data Processing System", shall come into force on 1 January 2001.

2. The institutions and persons referred to in Section 21 of this Law, which have commenced operations before the coming into force of this Law, shall register with the Data State Inspectorate by 1 March 2003. After expiry of this term, unregistered systems shall cease operations.
[24 October 2002]

3. Amendments (wording of 24 October 2002) to Section 4 shall come into force on 1 July 2003, but amendments to Section 29, Paragraph one shall come into force on 1 January 2004.
[24 October 2002; 1 March 2007]

4. Personal data processing systems, which until 28 November 2002 the law has not imposed a duty to register with the Data State Inspectorate, shall be registered by 1 July 2003.
[24 October 2002; 1 March 2007]

5. Administrators who have registered personal data processing systems until 1 September 2007, shall submit additional information free of charge to the Data State Inspectorate until 1 March 2008 to ensure the conformity of the information regarding processing of personal data with the requirements laid down in Section 22 of this Law.
[1 March 2007]

6. Until 1 March 2008 the Data State Inspectorate shall exclude from the register of processing of personal data those registered personal data processing systems the registration of personal data included therein is not stipulated in this Law and if any of the cases provided for in Section 22, Paragraph six of this Law has set in.
[1 March 2007]

7. Until 31 December 2010 the Data State Inspectorate shall exclude from the register of processing of personal data such registered processing of personal data the registration of

which is not stipulated in this Law.
[12 June 2009]

8. Amendments to Section 3, Paragraph two of this Law laying down the requirements for an authorised representative and obligation to inform the Data State Inspectorate regarding appointment of the authorised representative shall come into force from 1 December 2014.
[6 February 2014]

9. Until 1 June 2014 the Cabinet shall issue the Cabinet Regulation referred to in Section 26, Paragraph $2.^{1}$ of this Law. Until the day of coming into force of the relevant Cabinet Regulation, but not later than until 1 June 2014 the Cabinet Regulation No. 1322 of 17 November 2009, Requirements for Audit Opinion Regarding Personal Data Processing in State and Local Government Institutions, shall be in force.
[6 February 2014]

Informative Reference to European Union Directive
[21 February 2008]

This Law contains legal norms arising from Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

This Law has been adopted by the *Saeima* on 23 March 2000.

President V. Vīķe-Freiberga

Rīga, 6 April 2000