

The Saeima has adopted and
the President has proclaimed
the following law

*(latest amendments on 21 June 2012
that came into force on 18 July 2012)*

Personal Data Protection Law

*(Unofficial translation; the English language text
of the Personal Data Protection Law is provided for information only.)*

Chapter I

General Provisions

Article 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, regarding the processing of natural person data (hereinafter - personal data).

Article 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, clearly expressed affirmation of will 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 controller in accordance with Article 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, utilisation, transfer, transmission and dissemination, blockage or erasure;
- 5) **personal data processing system** - a structured personal data set recorded in any format that is accessible considering relevant identification criteria of the person;
- 6) **personal data processor** - a person authorised by the data controller, who carries out personal data processing on behalf of the data controller.
- 7) **recipient of personal data** - a natural or a legal person to whom personal data are disclosed;

8) **sensitive personal data** - personal data that indicate the race, ethnic origin, religious, philosophical or political convictions, or trade union membership of a person, or provide information as to the health or sexual life of a person;

9) **data controller** - a natural or a legal person, state or local government institution that determines the purposes and the means of personal data processing as well as is responsible for the processing of personal data in accordance with this Law;

10) **third person** - any natural or legal person, except for the data subject, the controller, the personal data processor and persons who have been directly authorised by the controller or the personal data processor.

11) **identification code of the person**- a number that is allocated for the identification of the data subject.

(With the amendments to the Law on 24.10.2002. and the amendments on 01.03.2007. that came into force on 01.09.2007.)

Article 3

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

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

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

3) the equipment is located in the territory of the Republic of Latvia that is used for the processing of personal data, except the cases when the equipment is used only for the transmission of personal data through the territory of the Republic of Latvia.

(2) In the cases referred to in Paragraph one, Clause 3 of this Article, the controller appoints an authorised person who is responsible for the compliance with this Law.

(3) This Law does not apply to the personal data processing performed by natural persons for personal or household and family purposes, furthermore the personal data collected are not disclosed to other persons.

(24 October 2002 and 1 March 2007 (in force since 1 September 2007)).

Article 4

This Law regulates the protection of those personal data that have been declared as official secret objects, taking into account the exceptions specified in "The Law On Official Secrets".

[24 October 2002; see Transitional provisions]

Article 5

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

(2) In applying the provisions of Paragraph one of this Article the rights of persons to inviolability of private life and freedom of expression shall be observed.

[1 March 2007 (in force since 1 September 2007)]

Chapter II

General Principles for Personal Data Processing

Article 6

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

Article 7

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

- 1) there is a consent of data subject;
- 2) the personal data processing derives 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 conclude the relevant contract;
- 3) the data processing is necessary for the controller to perform his duties as specified by law;
- 4) the data processing is necessary to protect vitally important interests of the data subject, including life and health;
- 5) the data processing is necessary in order to ensure that the public interest is complied with or to fulfil functions of public authority for whose performance the personal data have been transferred to the controller or transmitted to a third person;
- 6) the data processing is necessary in order to comply with the fundamental human rights and freedoms of the data subject, exercise lawful interests of the controller or of such third person to whom the personal data have been disclosed to.

[24 October 2002; 1 March 2007, in force since 1 September 2007]

Article 8

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

- 1) the title or name and surname, and the address of the data controller and the personal data processor;

2) the intended purpose and basis for the personal data processing.

(2) Based on the request from the data subject, the data controller 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 the access to his or her personal data and to make corrections to such data;

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

(3) Paragraph one of this Article is not applicable if carrying out personal data processing without disclosing its purpose is authorised by law.

[24 October 2002; 1 March 2007, in force since 1 September 2007]

Article 9

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

1) the title or the name, surname, and address of the data controller and the personal data operator;

2) the intended purpose for the personal data processing.

(2) Based on the request from the data subject, the data controller has a duty to provide the following information:

1) the possible recipients of the personal data;

2) the personal data categories and the source of obtaining the data;

3) the right of data subject to gain access to his or her personal data and of making corrections to such data.

(3) Paragraph one and two of this Article is not applicable, if:

1) the law provides for the processing of personal data without informing the data subject thereof;

2) when processing personal data for scientific, historical or statistical research, or the establishment of Latvian National Archive foundation, the informing of the data subject requires disproportionate effort or is impossible.

(Amendments to law of 24.10.2002, with the amendments of 01.03.2007. and 21.06.2012. that came into force on 18.07.2012.)

Article 10

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

- 1) the personal data are processed fairly and lawfully;
- 2) the personal data are processed only in conformity with the intended purpose and to the extent required therefore;
- 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 accuracy of personal data and their timely update, rectification and deletion, if 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 indicated 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 Article 9 and Article 10, Paragraph one of this Law.

(3) Paragraph one, Clauses 3 and 4 of this Article are not applicable to the processing of personal data for the establishment of Latvian National Archive foundation according to the procedures specified in regulatory enactments.

(4) Personal data processing within the area of criminal law for purposes other than those originally indicated is permissible:

- 1) in order to prevent, disclose, and investigate criminal offence and to carry out criminal prosecution or to impose criminal punishment;
- 2) in order to use personal data for administrative and civil court proceedings, as well as for the operation of the state institutions or state officials that are authorised by the law if it is related to the prevention, disclosure, investigation or criminal prosecution, or imposing of criminal fine;
- 3) in order to prevent essential threats to the public security;
- 4) if data subject has provided consent for personal data processing.

(With the amendments of 24.10.2002., 01.03.2007.; 06.05.2010., and 21.06.20012 with the law that came into force on 18.07.2012.)

Article 11

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

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

- 2) special processing of personal data, without requesting the consent of the data subject, is provided for by regulatory enactments, which regulate legal relations regarding employment, and such regulatory enactments guarantee the protection of personal data;
- 3) personal data processing 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) personal data processing is necessary to achieve the lawful, non-commercial objectives of nongovernmental organisations and their associations, if such data processing is only related to the members of these organisations or their associations and the personal data are not transferred to third parties;
- 5) personal data processing is necessary for the purposes of medical treatment, for provision or the administration of health care services and the distribution or the administration of medicine and medical devices;
- 6) the processing concerns such personal data as necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings;
- 7) personal data processing is necessary for the provision of social assistance and it is performed by the provider of social assistance services;
- 8) personal data processing is necessary for the establishment of Latvian National Archive foundation and it is performed by the State Archives and institutions with state storage rights approved by the Director-general of the State Archives;
- 9) personal data processing is necessary for statistical research that is carried out by the Central Statistics Bureau;
- 10) the processing relates to such personal data that the data subject has him or herself made public;
- 11) personal data processing is necessary for the performance of state administration functions or for the development of the state information systems determined by the law;
- 12) personal data processing is necessary for the natural or legal person's rights or legitimate interests, by requiring compensation according to the insurance contract;
- 13) according to the Law on the Rights of Patients, for the research patients data are used from the recorded medical documents.

(With the amendments that came into force on 18.07.2012.)

Article 12

Personal data that relate to the commitment of criminal offences, convictions in criminal matters and administrative violations cases, as well as to the court decision or court case file, only persons authorised by law are entitled to process such data and in the cases specified by the law.

[1 March 2007, in force since 1 September 2007]

Article 13

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

(2) Personal data may be disclosed based on a written request or agreement, indicating the purpose for the use of the data, if not prescribed otherwise by law. In the request for personal data, the information shall be indicated that allows identifying the personal data requester 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 have been foreseen.

[1 March 2007, in force since 1 September 2007]

Article 13¹ Personal identification (classification) 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 personal data processing;

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 Data State Inspectorate.

[1 March 2007, in force since 1 September 2007]

Article 14

(1) The data controller may entrust personal data processing to the personal data processor by concluding a written agreement.

(2) The 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 data controller if they are not in conflict with regulatory enactments.

(3) Prior to commencing personal data processing, the personal data processor shall carry out security measures for personal data processing determined by the data controller for the protection of the system in accordance with the requirements of this Law.

[24 October 2002; 1 March 2007, in force since 1 September 2007]

Chapter III

Rights of Data Subject

Article 15

(1) In addition to the rights referred to in Articles 8 and 9 of this Law, the data subject has the right to obtain all the information that has been collected concerning him or her in any personal data processing system, unless the disclosure of such information is prohibited by law in the field of national security, defence and criminal law or for the purpose of ensuring the financial interests of the state in tax collection matters.

(2) The data subject has the right to obtain the information concerning those natural or legal persons who within a prescribed time period have received information from the data controller concerning this data subject. In the information to be provided to the data subject, it is prohibited to include state institutions that administer criminal procedures, carry out investigative field work, or other institutions concerning which the disclosure of such information is prohibited by law.

(3) The data subject also has the right to request the following information:

1) the title or name, surname, and address of the data controller;

2) the purpose, amount and method of the personal data processing;

3) the date when the personal data concerning the data subject were last rectified, data deleted 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 utilised concerning the automated processing systems, concerning the application of which the individual automated decisions are taken.

(4) The data subject has the right, within a period of one month from the date of submission of the relevant request (not more frequently than two times a year), to receive the information specified in this Article in writing free of charge.

(With the amendments to the Law on 24.10.2002., 01.03.2007., 21.02.2008. and 21.06.2012 that came into force on 18.07.2012.)

Article 16

(1) The data subject has the right to request that his or her personal data are supplemented or rectified, as well as that their processing would be suspended 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 justify that the personal data are incomplete, outdated, false, unlawfully obtained or no longer necessary for the purposes for which they were collected, the data controller has an obligation

to rectify this inaccuracy or violation without delay and notify third parties who have previously received such processed personal data.

(2) [Excluded on 1 March 2007].

(3) The data subject has the right to receive from the data controller a written and grounded answer regarding the considered request within one month since the request was submitted.

[1 March, 2007; 12 June 2009]

Article 17

Articles 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 national documentary heritage in accordance and based on regulatory enactments, where regarding the data subject no activities are carried out and no decisions are taken regarding the data subject.

(With the amendments of 24.10.2002. and 21.06.2012. that came into force on 18.07.2012.)

Article 18

If the data subject disputes an individual decision that has been taken only based on the automated data processing, and creates, amends, determines or terminates legal relations, the data controller has a duty to review it. The data controller may refuse to review such a decision if it has been taken based on the law or based on the contract that has been concluded with the data subject.

[24 October 2002; 1 March 2007, in force since 1 September 2007]

Article 19

The data subject has the right to prohibit the processing of his or her personal data for commercial purposes in cases referred to in the Article 7, Clause 6 of this Law, for their use regarding information society services, market and public opinion research, genealogical research, except in cases where the law provides otherwise.

[1 March 2007, in force on 1 September 2007]

Article 20

If the data controller fails to respect the obligations determined in this Law, the data subject has the right to appeal to Data State Inspectorate the refusal of the data controller to provide the information referred to in the Article 15 of this Law or perform the activities referred to in Article 16 of this Law, attaching the documents as the approval that the data controller refuses or fails to perform the obligations determined by the law.

[12 June 2009]

Chapter III¹

Data Subject Rights regarding to Personal data Processing in Eurojust and European Police Office

(Chapter in the edition of the amendments to the Law of 21.06.2012. that came into force on 18.07.2012.)

Article 20.¹

Data subject has rights to submit a request to Data State Inspectorate regarding his or her personal data processing or regarding investigation of his or her personal data processing in Eurojust and European Police Office.

Article 20.²

Once receiving the requests for information according to the Article 20.¹ of this law, Data State Inspectorate without due delay but not later than within one month from the day when the request has been received, sends the request accordingly to Eurojust or European Police Office for consideration and informs about it the data subject.

Chapter IV

Notification and Protection of Personal Data Processing

(Title of this chapter according to the amendments of 1 March 2007, in force since 1 September 2007).

Article 21

(1) All state and local government institutions, the natural persons and legal persons that carry out or wish to commence the personal data processing, notify it in the order determined by this law;

(2) The notification procedure prescribed by this Law is not applicable to personal data processing:

- 1) for the purposes of bookkeeping and personnel record keeping;
- 2) for the information systems of state and local government institutions when the data gathered there are publically available;
- 3) for journalistic purposes in accordance with the Law on Press and Other Mass Media;
- 4) for management of documents and archive in accordance with the Law on the Archives;
- 5) if it is carried out by religious organizations;
- 6) if the data controller has registered the personal data protection officer in accordance with the procedures prescribed in this Law;

7) if the data processing is carried out in accordance with the Article 7, Clause 1 and 2, or Article 13¹;

8) it is carried out for scientific, statistical and genealogical research purposes.

(3) The exemptions referred to in Paragraph 2 of this Article are not applicable if:

1) it is foreseen to transfer personal data to the country that is not Member State of the European Union or the European Economic Area;

2) it is foreseen to process personal data in relation with the provision of financial services, market or public opinion research, selection or evaluation of personnel as entrepreneurship if it is provided as a service to other companies/ state institutions/ natural persons, raffling or lotteries;

3) the information on person's health is processed;

4) personal data processing relates to criminal offenses, criminal records in criminal and administrative violation cases.

(With the amendments of 01.03.2007., 12.06.2009., 06.05.2010. and 21.06.2012 that came into force on 18.07.2012.)

Article 21¹

(1) The data controller may not notify personal data processing, if he or she designates the personal data protection officer. Personal data protection officer is not personal data processor.

(2) A natural person can be assigned as personal data protection officer who has higher education in jurisprudence, information technology or similar field and who has been trained according to the order specified by the Cabinet of Ministers.

(3) The data controller grants the necessary tools for the personal data protection officer, provides the necessary information and foresees the time within the working hours when the officer could perform also the duties of personal data protection officer.

(4) The data controller shall register the personal data protection officer in Data State Inspectorate.

(5) The register of personal data protection officers is publicly available. The following information on personal data protection officers is indicated in the register:

1. the name and surname of the person, contact information (address, telephone number, e-mail address);

2. the period for which the person is appointed;

3. the place of personal data processing and information on the possibilities to receive the information referred to in the Article 22, Paragraph 1 of this Law.

(6) Data State Inspectorate may postpone the registration of personal data protection officer, if all the information referred to in Paragraph 5 of this Article is not submitted.

(7) Data State Inspectorate does not register the personal data protection officer, if:

- 1) he or she does not meet the requirements of this Law;
- 2) one of the cases referred to in Article 22 of this Law has occurred.

(8) Data State Inspectorate excludes the personal data protection officer from the register in the following cases where:

- 1) the application from the controller on exclusion of the personal data protection officer from the register has been received;
- 2) in the period of one month after the registration of personal data protection officer the controller has not submitted an application for the exclusion of the personal data processing from the Register of Personal Data Processing.

(9) Data State Inspectorate takes the decision on the registration of the personal data protection officer within 15 days after all of the information referred to in Paragraph 5 of this Article has been submitted to Data State Inspectorate.

(10) Data State Inspectorate may exclude the personal data protection officer from the register and request the registration of personal data processing in accordance with Article 22 of this Law, if Data State Inspectorate concludes the violations of this Law regarding personal data processing that is in competence of the personal data protection officer.

[1 March 2007, 12 June 2009].

Article 21.²

(1) The personal data protection officer organizes, controls and supervises the compliance of the personal data processing carried out by the data controller with the requirements of this law.

(2) Personal data protection officer creates the register where the information referred to in Paragraph 1, Article 22 of this Law is entered (except the information referred to in the Paragraph 1, Clause 10 and 11, of the same Article), which on the request of data subject or Data State Inspectorate shall be provided free of charge.

(3) The obligation of the personal data protection officer is to retain and not disclose without the legal ground the personal data also after the termination of the employment relationship or resigning from the office.

(4) The personal data protection officer prepares the annual report on his or her activities and submits it to the data controller annually.

[1 March 2007, 12 June 2009.]

Article 22

(1) The institutions and persons referred to in the Article 21 of this Law which wish to commence personal data processing shall submit a notification application to Data State Inspectorate that includes the following information:

- 1) the name, surname, and personal code (for legal person - the title and the registration number), address and telephone number of the data controller;
- 2) the name, surname, and personal code of the personal data processor (if applicable), address and telephone number (for legal persons - the title and the registration number);
- 3) the legal basis for the personal data processing;
- 4) the types of personal data and the purposes of personal data processing;
- 5) the categories of data subjects;
- 6) the categories of personal data recipients;
- 7) the intended method of personal data processing;
- 8) the foreseen method of personal data obtaining;
- 9) the place of personal data processing;
- 10) the holder of information resources or technical resources, as well as the responsible person for the information system security;
- 11) technical and organisational measures ensuring the protection of personal data;
- 12) what personal data will be transferred to other countries, that are not the Member States of the European Union or European Economic Area.

(2) Data State Inspectorate shall identify the personal data processing where the risks regarding the data subjects' rights and freedoms are feasible. For such personal data processing the prior checking is determined.

(3) When notifying the personal data processing, Data State Inspectorate shall issue a certificate of the personal data processing notification to the controller or to his or her authorised person.

(4) Prior to making the changes to the personal data processing, such changes shall be notified to Data State Inspectorate except the information referred to in the Paragraph one, Clause 11 of this Article.

(5) If the technical and organisational measures of the personal data processing are changed that significantly impact the protection of the personal data processing, information regarding it shall be submitted within a period of one year to Data State Inspectorate.

(6) If the data controller changes or the operation of the data controller is terminated, he shall submit to Data State Inspectorate the application on the exclusion of the personal data processing from the Register of the Personal Data Processing.

(7) Data State Inspectorate shall take a decision on the data controller's exclusion from the Register of the Personal Data Processing, as well as on annulling the notification certificate of the personal data processing if:

1) the data controller has not prevented the breaches within the time limit specified by Data State Inspectorate;

2) the data controller has not submitted to Data State Inspectorate the notification on the changes regarding the personal data processing within one month after the changes of personal data processing have been made or has not submitted the application referred to in the Paragraph 6 of this Article.

(8) The Cabinet of Ministers determines the following samples of application forms:

1) application on the notification of the personal data processing;

2) application on the notification of the amendments regarding the personal data processing;

3) application on the registration of the personal data protection officer;

4) application on the exclusion of the personal data processing from the Register of the Personal Data Processing;

5) application on the exclusion of the personal data protection officer from the register of Data State Inspectorate.

(9) For the notification of each personal data processing or the notification of the changes referred to in Paragraph four of this Article, a state tax shall be paid according to the procedures and in the amount specified by the Cabinet of Ministers.

(Amendments of 1 March 2007, in force since 1 September 2007.)

Article 23

(1) Data State Inspectorate may postpone the registration of personal data processing or the decision on the registration of amendments to the personal data processing, if:

1) the deficiencies are concluded regarding the notification form of the personal data processing;

2) all of the information referred to in Article 22 of this Law is not submitted;

3) the state tax has not been paid.

(2) Data State Inspectorate shall not register the notification of the personal data processing or may take a decision on refusal to register the amendments regarding personal data processing, if:

1) within the time limit of 30 days the data controller has not prevented the deficiencies identified and reported by Data State Inspectorate;

2) the application form for notification of the personal data processing or notification of amendments to the personal data processing is submitted by the person who shall not be considered as the data controller according to this law;

3) on inspection of the personal data processing, the breaches of legal acts are determined regarding personal data protection.

(3) Submitting the documents repeatedly, after the time limit set in this law for prevention of deficiencies identified in the documents, the applicable state tax should be paid repeatedly.

(4) In cases determined in Paragraph two, Clause 2 of this Article, state tax shall be refunded in accordance with decision of Data State Inspectorate.

(Amendments of 1 March 2007, in force since 1 September 2007.)

Article 24

(1) Data State Inspectorate shall include the information referred to in the Paragraph one and four of the Article 22 of this Law in the Register of the Personal Data Processing, except the information referred to in the Paragraph two, Clause 10 and 11 of this Article. The register is publicly available.

(2) In the register mentioned in the Paragraph one of this Article the information on the personal data processing shall not be included that is regulated by the Law On Official Secrets and the Investigatory Operations Law.

(Amendments of 1 March 2007, in force since 1 September 2007.)

Article 24¹

The registers referred to in the Paragraph five of Article 21¹ and Paragraph one of Article 24 of this law are the component parts of the personal data processing supervision information system. The personal data processing supervision information system is the state information system; its operation is organized and administered by Data State Inspectorate.

(Amendments of 1 March 2007, in force since 1 September 2007.)

Article 25

(1) The obligation of the data controller and the personal data processor is to use the necessary technical and organizational measures in order to protect the personal data and to prevent their unlawful processing.

(2) The data controller shall control the form of personal data recorded and the time of recording and is responsible for the actions of those persons who carry out personal data processing.

(Amendments of 24 October 2002; 1 March 2007, in force since 1 September 2007.)

Article 26

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

(2) Once in two years state and local government institutions shall submit to Data State Inspectorate the audit reports on personal data processing, including the risk analysis and a report regarding measures implemented in the field of the information security. The requirements for audit report shall be determined by the Cabinet of Ministers.

(3) and (4) [Excluded on 12 June 2009]

(24 October 2002, 19 December 2006, 1 March 2007, amendments of 12 June 2009 that came into force on 01.07.2009.)

Article 27

(1) Natural persons involved in personal data processing shall make a commitment in writing to preserve and not disclose the personal data in an unlawful manner. Such persons have a duty not to disclose the personal data even after the termination of the legal employment relationships or other contractually specified relations.

(2) The data controller is obliged to keep a record of the persons referred to in the Paragraph one of this Article.

(3) When processing the personal data, the processor of the personal data shall comply with the instructions of the data controller.

(Amendments of March 2007, in force since 1 September 2007.)

Article 28

(1) Personal data may be transferred to another country that is not the member state of the European Union or the European Economic Area, if that country ensures such level of data protection that corresponds to the relevant level of the data protection that is in force in Latvia.

(2) Exemptions from compliance with the requirements referred to in the Paragraph one of this Article are permissible if the data controller undertakes to perform the supervision regarding the performance of the relevant protection measures and at least one of the following conditions is complied with:

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

2) the transfer of the data is necessary in order to fulfil an agreement between the data subject and the controller, the personal data are required to be transferred in accordance with contractual obligations binding upon the data subject or 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 necessary and requested pursuant to the prescribed procedures, in accordance with significant state or public interests, or is required for the legal 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 that are public or have been stored in a publicly accessible register.

(3) The evaluation of the level of personal data protection in accordance with Paragraph one of this Article shall be performed by Data State Inspectorate and it shall issue a permission in writing for the transfer of the personal data.

(4) In order for the data controller to ensure the supervision on the performance of the relevant protection measures in accordance with the Paragraph two of this Article, the data controller and the personal data receiver shall conclude the agreement on the personal data transfer. The requirements for the mandatory provisions for this contract shall be determined by the Cabinet of Ministers. The agreement regarding personal data transfers is not concluded in the areas of international cooperation, national security and criminal law.

(5) Personal data can be transferred to the other member state of European Union or the European Economic Area if that country ensures such level of data protection as corresponds to the relevant level of the data protection in force in Latvia.

(6) Once transferring personal data to another country or international organisation, the foreseen restrictions regarding personal data processing are notified, unless they are included in the agreement mentioned in Paragraph four of this article.

(With the amendments of 24.10.2002., 01.03.2007., and 06.05.2010 that came into on 02.06.2010.)

Article 29

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

(2) Data State Inspectorate shall act in accordance with its bylaws approved by the Cabinet of Ministers. Every year Data State Inspectorate shall submit a report on its activities to the Cabinet of Ministers and shall publish it in the newspaper *Latvijas Vēstnesis*.

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

- 1) to ensure the compliance of personal data processing in the country with the requirements of this Law;
- 2) to take decisions and review complaints regarding the protection of personal data;
- 3) to register the personal data processing;
- 4) to propose and carry out activities aimed at raising the effectiveness of personal data protection and provide opinions on the conformity of personal data processing systems to be established by the state and local government institutions to the requirements of regulatory enactments;
- 5) [Excluded on 21 June 2012].
- 6) [Excluded on 12 June 2009].

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

- 1) in accordance with the procedures prescribed by regulatory enactments, to receive free of charge the necessary information from the natural persons and legal persons for the performance of functions pertaining to inspection;
- 2) to perform an investigation of a personal data processing;
- 3) to demand blocking the data, to request the deletion or destruction of the inaccurate or unlawfully obtained data, or to demand a permanent or temporary prohibition of data processing;
- 4) to bring an action to court for violations of this Law;
- 5) to annul the personal data processing notification certificate if by investigating the personal data processing violations are concluded;
- 6) to impose administrative penalties according to the procedures specified by law regarding violations of personal data processing;
- 7) to perform the inspections in order to determine the conformity of personal data processing to the requirements of regulatory enactments in cases when it is prohibited by law to the data controller to provide information to the data subject and the relevant request from the data subject has been received.

(With the amendments of 24.10.2002., 01.03.2007., 12.06.2009., and 21.06.2012 that came into force on 18.07.2012.)

Article 30

(1) In order to perform the duties referred to in Article 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 personal data processing is carried out, and in the presence of the representative of the controller carry out the necessary inspection or other measures in order to determine the compliance of the personal data processing procedure with the law;
- 2) to require written or verbal explanations from any natural or legal person involved in personal data processing;
- 3) to require that documents are presented and other information is provided that relates to the personal data processing being inspected;
- 4) to require inspection of a personal data processing, any equipment or information carrier of personal data, and to determine an expert's examination to be conducted regarding questions subject to investigation;
- 5) to request assistance of officials of law enforcement institutions or other specialists, if necessary, 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 necessary;
- 7) to draw up administrative violation report regarding administrative violations case regarding the personal data processing.

(2) The officials of 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 the information that is publicly accessible. Such prohibition shall also remain in effect after the officials have ceased to fulfil their official duties.

(Amendments of 24 October 2002; 1 March 2007, in force since 1 September 2007.)

Article 30¹

Data State Inspectorate is the national supervisory institution that is carrying out the supervision of the national part of the Schengen Information System and carrying out the inspections regarding the personal data entered into the Schengen Information System, considering if they are processed not violating the rights of the data subject.

(Amendments of 1 March 2007, in force since 1 September 2007.)

Article 31

(1) The administrative act that is issued by the officials of Data State Inspectorate or their actual actions may be appealed to the director of Data State Inspectorate. The administrative act issued by the director of Data State Inspectorate or his/ her actual actions, as well as the

decision regarding the appealed administrative act or actual action can be may be appealed to the court in the order determined by court.

(2) The appeal or dispute regarding the decision of director of Data State Inspectorate or the decision of other officials regarding the blockage of data, permanent or temporary ban regarding data processing, does not stop the operation of this decision, except in the case, where it is suspended with a decision of the person examining the submission or application.

Article 32

Once violating this Law, harm or loss has been caused to the person; he or she has the right to receive compensation accordingly.

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 Article 21 of this Law that have commenced their operations before this Law came into force, shall notify to Data State Inspectorate by 1 March 2003. After expiry of this term, non-notified systems shall cease operation.

(Amendments of 24 October 2002.)

3. Amendments to Article 4 shall come into force on 1 July 2003, but the amendments (24 October 2002) to the Article 29, Paragraph one shall come into force on 1 January 2004.

(Amendments of 24 October 2002; 1 March 2007, in force on 1 September 2007.)

4. Personal data processing systems, which this law did not oblige to notify to Data State Inspectorate until 28 November 2002, shall be notified by 1 July 2003.

(Amendments of 24 October 2002; 1 March 2007, in force on 1 September 2007.)

5. The data controllers that have notified personal data processing systems until 1 September 2007 shall submit to Data State Inspectorate, free of charge, additional information, to ensure the compliance of information on personal data processing in accordance with provisions determined in Article 22 of this law.

(Amendments of 1 March 2007, in force since 1 September 2007.)

6. Data State Inspectorate until 1 March 2008 shall exclude personal data processing systems which contain personal data from the Register of Personal Data Processing that this law does not foresee to be notified, also regarding those cases when one of the cases prescribed in the Article 22, Paragraph six of this law has occurred.

(Amendments of 1 March 2007, in force since 1 September 2007.)

7. Data State Inspectorate until 31 December 2010 shall exclude from the Register of the Personal Data Processing those processings whose notification is not foreseen by this law.

(Amendments of 12.06.2009. that came into force on 01.07.2009.)

Informative Reference to European Union Directive

(Amendments of 21.02.2008. that came into force on 6 March 2008)

The legal provisions deriving from the 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 are incorporated in this law.

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

President V. Vike-Freiberga

Riga, 6 April 2000