UNOFFICIAL TRANSLATION

Text consolidated by Tulkosanas un terminologijas centrs (Translation and Terminology Centre) with amending laws of:
24 October 2002;
19 December 2006.
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 system 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, utilisation, 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 a system administrator, who carries out personal data processing upon the instructions of the system 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 provide information as to the health or sexual life of a person;

9) **system administrator** – a natural person or a legal person who determines the purposes and the means of processing of a personal data processing system; and

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

[24 October 2002]

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 system 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; and

3) in the territory of the Republic of Latvia is located equipment, which is utilised for the processing of personal data.

(2) In the cases referred to in Paragraph one, Clause 3 of this Section, the system administrator shall appoint an authorised person who shall be responsible for compliance with this Law.

(3) This Law shall not apply to the information systems made by natural persons in which personal data are processed for personal or household and family purposes and in which the personal data collected are not disclosed to other persons.

[24 October 2002]

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 and 11 of this Law shall not apply if personal data are processed for journalistic, artistic or literary purposes, and it is not prescribed otherwise by law.

(2) In applying the provisions of Paragraph one of this Section, regard shall be had to the rights of persons to inviolability of private life and freedom of expression.

Chapter II
General Principles for Personal Data Processing

Section 6.

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

Section 7.

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

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

2) the personal data processing 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 data processing is necessary to a system administrator for the performance of his or her 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 a system administrator or transmitted to a third person; and

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

[24 October 2002]

Section 8.

(1) When collecting personal data from a data subject, a system 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 system administrator and the personal data operator; and

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

(2) On the basis of a request from the data subject, the system administrator has a duty to provided 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; and

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 Section is not applicable if the conducting of personal data processing without disclosing its purpose is authorised by law.

[24 October 2002]

Section 9.

(1) If personal data have not been obtained from the data subject, a system administrator 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 designation, or given name and surname, and address of the system administrator and the personal data operator; and

2) the intended purpose for the personal data processing.

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

1) the possible recipients of the personal data;

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

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

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

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

2) when processing personal data for scientific, historical or statistical research, or the establishment of Latvian national archive holdings, the informing of the data subject requires inordinate effort or is impossible.

[24 October 2002]

Section 10.

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

1) the personal data processing 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; and

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 Latvian national archive holdings according to the procedures specified in regulatory enactments.

[24 October 2002]

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 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 public 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, the provision of health care services or the administration thereof and the distribution of means of medical treatment;

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 holdings 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, which is performed by the Central Statistics Bureau; and

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

[24 October 2002]

Section 12.

If personal data, which relate to the commitment of criminal offences, convictions in criminal matters, court proceedings in criminal matters and closed court sittings in civil matters, only persons authorised by law are entitled to process such data and in the cases specified by law.

[24 October 2002]

Section 13.

(1) A system administrator is obliged to disclose personal data in cases provided for by law to officials of State and local government institutions. The system 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.

Section 13.[1]

Personal identification (classification) codes may be processed if:

1) the consent of the data subject has been received;

2) the processing of the identification (classification) codes arises from the purpose of the personal data processing;

3) the processing of the identification (classification) codes is necessary to ensure the continuing anonymity of the data subject; and

4) a written permit has been received from the Data State Inspectorate.

[24 October 2002]

Section 14.

(1) A system administrator may entrust personal data processing 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 system administrator if they are not in conflict with regulatory enactments.
(3) Prior to commencing personal data processing, a personal data processor shall perform safety measures determined by the system administrator for the protection of the system in accordance with the requirements of this Law.
[24 October 2002]

Chapter III
Rights of a Data Subject

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 system for personal data processing, unless the disclosure of such information is prohibited by law in the field of national security, defence and criminal law.
(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 a system 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 system administrator;
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 extinguished or blocked;
4) the source from which the personal data were obtained unless the disclosure of such information is prohibited by law; and
5) the processing methods utilised for the automated processing systems, concerning the application of which individual automated decisions are taken.
(4) A 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 Section in writing free of charge.
[24 October 2002]

Section 16.

(1) A data subject has the right to request that his or her personal data be supplemented or rectified, as well as that their processing be suspended or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully obtained 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 included in the personal data processing system are incomplete, outdated, false, unlawfully obtained or no longer necessary for the purposes for which they were collected, the system administrator has an obligation to rectify this inaccuracy or violation without delay and notify third parties who have previously received the processed data of such.
(2) If information has been retracted, a system administrator shall ensure the accessibility of both the new and the retracted information, and that the information referred to is received simultaneously by recipients thereof.

Section 17.

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 Latvian national archive holdings in accordance with

regulatory enactments and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject.
[24 October 2002]

Section 18.

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 system administrator has a duty to review such data. The system 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.
[24 October 2002]

Section 19.

A data subject has the right to object to the processing of his or her personal data if such will be used for commercial purposes.

Section 20.

A data subject has the right to appeal to the Data State Inspectorate the refusal of a system administrator to provide the information referred to in Section 15 of this Law or perform the activities referred to in Section 16 of this Law.

Chapter IV
Registration and Protection of a Personal Data Processing System

Section 21.

(1) All State and local government institutions, and other natural persons and legal persons which carry out or wish to commence carrying out personal data processing, and establish systems for personal data processing, shall register such in accordance with the procedures prescribed in this Law unless otherwise prescribed by law.
(2) The registration procedure prescribed by this Law is not applicable to personal data processing for the needs of accounting and personnel registration if the personal data is not being accumulated in electronic form, as well as on the personal data processing systems established by the denominational religious organisation referred to in the Civil Law.
[24 October 2002]

Section 22.

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

1) the designation (name and surname), registration code, address and telephone number of the institution or person (system administrator);

2) the name, surname, personal identity number, address and telephone number of a person authorised by the system administrator;

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

4) the type of personal data to be included in the system, the purposes for which it is intended and the amount of personal data to be processed;

5) the categories of data subjects;

6) the categories of recipients of personal data;

7) the intended method of personal data processing;

8) the planned method of obtaining personal data and a mechanism for the control of their quality;

9) other data processing systems, which will be connected with the system to be registered;

10) what personal data connected systems will be able to obtain from the system to be registered, and

what data the system to be registered will be able to obtain from connected systems;

11) the method for transferring data from the system to be registered to another system;

12) the identification codes of natural persons as will be used by the system to be registered;

13) the method for exchanging information with the data subject;

14) the procedures whereby a personal data subject is entitled to obtain information concerning himself or herself and other information referred to in Sections 8 and 9 of this Law;

15) the procedures for supplementing and updating of personal data;

16) technical and organisational measures ensuring the protection of personal data; and

17) what personal data will be transferred to other states.

(2) The Data State Inspectorate shall evaluate and determine the personal data processing systems in which a prior checking must be performed.

(3) When registering a personal data processing system, the Data State Inspectorate shall issue a certificate of registration of the personal data processing system to a system administrator or to a person authorised by him or her.

(4) Prior to changes being made in a personal data processing system, such changes shall be registered in the Data State Inspectorate if the following changes:

1) the system administrator or the personal data processor;

2) the location of the personal data processing system;

3) the types of personal data or the purpose of the personal data processing;

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

5) the data processing systems with which the relevant system is associated;

6) the type of personal data processing; and

7) the type of personal data processing, which is transferred to other states.

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

(6) For the registration of each personal data system 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 specified by the Cabinet.

[24 October 2002]

Section 23.

The Data State Inspectorate may refuse to register a personal data processing system, if:

1) all of the information referred to in Section 22 of this Law is not submitted; or

2) on inspection of the personal data processing system, violations are determined.

Section 24.

(1) The Data State Inspectorate shall include the information referred to in Section 22 of this Law in the register for personal data processing systems (except the information referred to in Clause 16 of the same Section). The register is a component part of the State information system.

(2) Information regarding those registered personal data processing systems the operation of which is regulated 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.

[24 October 2002]

Section 25.

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

[24 October 2002]

Section 26.

(1) The mandatory technical and organisational requirements for the protection of personal data processing systems shall be determined by the Cabinet.
(2) Every year State and local government institutions shall submit to the Data State Inspectorate a personal data processing system internal audit findings (also a system risk analysis) and a report regarding measures performed in the field of information security.
(3) The Data State Inspectorate in accrediting a person who wishes to perform systems audits in State and local government personal data processing systems shall perform the following in relation to external systems auditors:

1) initial accreditation;
2) repeated accreditation;
3) accreditation for the renewal of activities;
4) extension of the time period of the accreditation; and
5) issuing of duplicates of accreditation certificates.

(4) For the performance of each of the activities referred to in Paragraph three of this Section, a State fee shall be paid according to the procedures and in the amount specified by the Cabinet.
[24 October 2002; 19 December 2006]

Section 27.

(1) Natural persons involved in personal data processing 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) A system 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 system administrator.

Section 28.

(1) Personal data may be transferred to another state if that state 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 system administrator undertakes to perform 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 consent to the transfer of the data to another state;
2) the transfer of the data is necessary in order to fulfil an agreement between the data subject and the system 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; or
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.
[24 October 2002]

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 regulatory enactments, 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 Vetsnesis* [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 ensure compliance of personal data processing in the State with the requirements of this Law;

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

3) to register personal data processing systems;

4) to propose and carry out activities aimed at raising the effectiveness of personal data protection and provide opinions regarding the conformity of personal data processing systems to be established by the State and local governments to the requirements of regulatory enactments;

5) together with the Office of the Director General of the State Archives of Latvia, to decide on the transfer of personal data processing systems to the State archives for preservation thereof; and

6) to accredit persons who wish to perform system audits of State and local government institution personal data processing systems according to the procedures specified by the Cabinet.

(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 regulatory enactments, 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 personal data processing system;

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 personal data processing registration certificate if in inspecting the personal data processing system violations are determined;

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

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

[24 October 2002]

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 personal data processing systems are located, and in the presence of a representative of the system administrator carry out necessary inspections or other measures in order to determine the compliance of the personal data processing procedure with 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 which relate to the personal data processing system being inspected;

4) to require inspection of a personal data processing system, 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; and

7) to draw up a statement regarding administrative violations in personal data processing.

(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]

Section 31.

Decisions by the Data State Inspectorate may be appealed to a court.

Section 32.

If, in violating 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 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]

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

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

President V. Vike-Freiberga

Riga, 6 April 2000