Personal Data Protection Law

The Saeima(i) 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 using data available within a data processing system;

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;

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 criteria;

6) processor of personal data — a person authorised by a system controller, who carries out personal data processing upon the instructions of the system controller;

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 controller — a natural or a legal person who manages a personal data processing system and determines its purposes and the means of processing;

10) third person — any natural or legal person except for a data subject, a system controller, a system processor and persons who have been directly authorised by a system controller or a processor of personal data.

Section 3.

(1) This Law applies to the processing of all types of personal data, and to any natural and legal person involved in personal data processing, except in the cases set out in Paragraphs two and three of this Section.

(2) This Law does 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.

(3) This Law does not apply to the processing of personal data carried out by public institutions in the fields of national security and criminal law.

Section 4.

The protection of personal data which have been declared to be official secret matters shall be regulated by the Law on Official Secrets.

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;

3) the data processing is necessary to a system controller for the performance of his or her lawful obligations;

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 controller 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 controller or of such third person as the personal data have been disclosed to.

Section 8.

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

1) the designation, or name and surname, and address of the system controller;

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

3) the possible recipients of the personal data;

4) the rights of the data subject to gain access to his or her personal data and the possibility of rectifying such data; and

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

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

Section 9.

(1) If personal data have not been obtained from the data subject, a system controller, prior to disclosing the data to third persons, is obliged to provide the data subject with the following information:

1) the designation, or name and surname, and address of the system controller;

2) the intended purpose for the personal data processing;

3) the possible recipients of the personal data;

4) the source of the personal data; and

5) the rights of data subjects to gain access to his or her personal data and the possibility of

rectifying such data.

(2) Paragraph one 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, the informing of the data subject requires inordinate effort or is impossible.

Section 10.

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

1) the personal data processing takes place lawfully;

2) the personal data are collected in accordance 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.

(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 mentioned in Section 9 and Section 10, Paragraph one of this Law.

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, is carried

out by a medical practitioner or a medical treatment institution and an adequate level of protection of personal data is ensured; or

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.

Section 12.

If personal data relate to disciplinary and administrative violations or judgments in civil matters, only officials authorised by State or local government institutions are entitled to process such data.

Section 13.

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

(3) The personal data received may be used only for the purposes for which they are intended.

Section 14.

(1) A system controller 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 scope determined in the contract and in accordance with the purposes provided for therein.

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

Chapter III. Rights of a Data Subject ➦

Section 15.

(1) In addition to the rights mentioned 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.

(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

controller 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 controller;

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

3) the date when the personal data concerning the data subject were last rectified;

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.

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 controller 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 controller shall ensure the accessibility of both the new and the retracted information, and that the information mentioned is received simultaneously by recipients thereof..

Section 17.

Section 15 and 16 of this Law are not applicable if the processed data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject.

Section 18.

A person is not required to comply with an individual decision which has been taken only upon the basis of data processed automatically. The person may be made subject to such aforementioned decision if it has been taken in accordance with law or a contract entered into with the data subject.

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 State Data Inspection the refusal of a system controller to provide the information mentioned in Section 15 of this Law or perform the activities mentioned 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 the personal data processing carried out in the areas of public safety, combating of crime or national security and defence, by institutions specially authorised by law.

Section 22.

(1) The institutions and persons mentioned 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 State Data Inspection which includes the following information:

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

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

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 scope 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 mentioned 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) Prior to registration of a personal data processing system, the State Data Inspection shall perform an inspection of the personal data processing system.

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

(4) Prior to changes being made to the information mentioned in Paragraph one of this Section, they shall be registered in the State Data Inspection.

Section 23.

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

1) all of the information mentioned 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 State Data Inspection shall include the information mentioned in Section 22 of this Law in the register for personal data processing systems. The register shall be accessible to the general public.

(2) Information concerning the registered personal data processing systems shall be published in accordance with the procedures prescribed in regulatory enactments.

Section 25.

(1) A system controller has an obligation to apply the necessary technical and organisational measures to protect personal data and prevent their illegal processing.

(2) A system controller 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.

Section 26.

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

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 controller is obliged to record the persons mentioned 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 controller.

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 and written consent has been obtained from the State Data Inspection.

(2) Exemption from compliance with the requirements of Paragraph one of this Section is permissible if 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 required to fulfil an agreement between the data subject and the system controller, or the personal data are required to be transferred in accordance with contractual obligations binding upon the data subject;

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.

Section 29.

(1) The protection of personal data shall be carried out by the State Data Inspection which shall be subject to the supervision of the Ministry of Justice. The State Data Inspection 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 State Data Inspection shall act in accordance with by-laws approved by the Cabinet. Every year the State Data Inspection shall submit a report on its activities to the Cabinet and shall publish it in the newspaper Latvijas Vetsnesis.

(3) The duties of the State Data Inspection 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

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.

(4) In the field of personal data protection, the rights of the State Data Inspection 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 prior to its registration;

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; and

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

Section 30.

(1) In order to perform the duties mentioned in Section 29, Paragraph three of this Law, the director of the State Data Inspection and the inspectors authorised by the director, upon presenting their official identification cards, 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 controller 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 produced 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, if required, in order to ensure performance of its duties; and

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

(2) The officials of the State Data Inspection 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.

Section 31.

Decisions by the State Data Inspection 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 mentioned in Section 21 of this Law, which have commenced operations before the coming into force of this Law, shall register with the State Data Inspection by 1 January 2002. After expiry of this term, unregistered systems shall cease operations.

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

President V. V__e-Freiberga

Riga, 6 April 2000

(i) The Parliament of the Republic of Latvia