REPUBLIC OF LITHUANIA

LAW

ON LEGAL PROTECTION OF PERSONAL DATA

11 June 1996 No I-1374

(As last amended on 3 November 2016 – No XII-2709)

Vilnius

CHAPTER ONE
GENERAL PROVISIONS

Article 1. Objective, Purpose and Scope of the Law

1. The purpose of this Law shall be safeguarding of the inviolability of an individual's private life in the course of processing personal data.

2. This Law shall regulate relations arising in the course of the processing of personal data by automatic means, and during the processing of personal data by other than automatic means in filing systems: lists, card indexes, files, codes, etc. The Law shall establish the rights of natural persons as data subjects, the procedure for protecting these rights, the rights, duties and liability of legal and natural persons while processing personal data.

3. This Law shall apply to the processing of personal data where:

1) personal data are processed by a data controller established and operating in the territory of Lithuania, as a part of activities thereof. Where personal data are processed by a branch office or a representative office of a data controller of a Member State of the European Union or another state of the European Economic Area, established and operating in the Republic of Lithuania, such a branch office or representative office shall be bound by the provisions of this Law applicable to the data controller;

2) personal data are processed by a data controller which is established in the territory other than the Republic of Lithuania, but which is bound by the laws of the Republic of Lithuania by virtue of international public law (including diplomatic missions and consular posts);

3) personal data are processed by a data controller established and operating in a country which is not a Member State of the European Union or another state of the European Economic Area (hereinafter: a 'third country'), where the data controller uses personal data processing means established in the Republic of Lithuania, with the exception of the cases where such

means are used only for transit of data through the territory of the Republic of Lithuania, the European Union or another state of the European Economic Area. In the case laid down in this point, the data controller must have its representative, that is, an established branch office or a representative office in the Republic of Lithuania which shall be bound by the provisions of this Law applicable to the data controller.

4. This Law shall not apply if personal data are processed by a natural person only for his personal needs not related to business or profession.

5. This Law shall not apply to the processing of personal data of deceased persons.

6. When personal data are processed for the purposes of state security or defence, this Law shall apply to the extent that other laws do not provide otherwise.

7. This Law shall not restrict or prohibit free movement of personal data when fulfilling European Union membership commitments of the Republic of Lithuania.

8. This Law shall harmonise regulation of legal protection of personal data in the Republic of Lithuania with the European Union legal acts referred to in the Annex to this Law.

Article 2. Definitions

1. **Personal data** shall mean any information relating to a natural person (data subject) who is known or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

2. **Data recipient** shall mean a legal or a natural person to whom personal data are disclosed. The authorities supervising the implementation of this Law referred to in Articles 8 and 36 of this Law as well as other state and municipal institutions and agencies shall not be regarded as data recipients when they obtain personal data in response to a specific request for the purposes of fulfilling their control functions laid down in laws.

3. **Disclosure of data** shall mean disclosure of personal data by transmission or making them available by any other means (with the exception of publishing them in mass media).

4. **Data processing** shall mean any operation, which is performed with personal data such as collection, recording, accumulation, storage, classification, grouping, combining, alteration (supplementing or rectifying), disclosure, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction or any other operation or a set of operations.

5. **Data processing by automatic means** shall mean any operation performed with personal data carried out in whole or in part by automatic means.

6. **Data processor** shall mean a legal or a natural person other than an employee of the data controller processing personal data on behalf of the data controller. The data processor

and/or the procedure of its/his nomination may be laid down in laws or other legal acts.

7. **Data controller** shall mean a legal or a natural person which alone or jointly with others determines the purposes and means of processing personal data. Where the purposes of processing personal data are laid down in laws or other legal acts, the data controller and/or the procedure for its/his nomination may be laid down in such laws or other legal acts.

8. **Special categories of personal data** shall mean data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life and criminal convictions.

9. **Prior checking** shall mean an advance inspection of processing data before it is started in the cases laid down in this Law.

10. **Social and public opinion survey** shall mean a systemic collection of data and/or information about natural and legal persons and interpretation thereof by means of statistical, analysis and other methods of social sciences with a view to obtaining insights required for decision-making. Direct marketing may not be undertaken when conducting a social and public opinion survey.

11. **Filing system** shall mean any structured set of personal data arranged in accordance with specific criteria relating to the person, allowing an easy access to personal data in the file.

12. **Consent** shall mean an indication of will given freely by a data subject indicating his agreement to the processing of his personal data for the purposes known to him. His consent with regard to special categories of personal data must be expressed clearly, in a written or equivalent form or any other form giving an unambiguous evidence of the data subject's free will.

13. **Direct marketing** shall mean an activity intended for offering goods or services to individuals by post, telephone or any other direct means and/or for obtaining their opinion about the offered goods or services.

14. **Third party** shall mean a legal or a natural person, with the exception of the data subject, the data controller, the data processor and persons who have been directly authorised by the data controller or the data processor to process data.

15. **Internal administration** shall mean activity which ensures an independent functioning of the data controller (structure administration, personnel management, management and use of available material and financial resources, and clerical work).

16. **Public data file** shall mean a state register or an information system or any other data file which, pursuant to laws of the Republic of Lithuania or other legal acts, is intended for the disclosure of data, information, documents and/or copies thereof to the public and which may be lawfully used by the public.

17. **Video surveillance** shall mean processing of image data concerning natural person

(hereinafter: ‘video data’) by using automated video surveillance means (video and photo cameras, etc.) irrespective of whether these data are recorded in a file or not.

18. The concepts of a credit institution and a financial institution shall be interpreted as they are defined in the Law on Financial Institutions.

CHAPTER TWO
PERSONAL DATA PROCESSING

Article 3. Requirements for the Processing of Personal Data

1. The data controller must ensure that personal data are:

1) collected for specified and legitimate purposes and later are not processed for purposes incompatible with the purposes determined before the personal data concerned are collected;

2) processed accurately, fairly and lawfully;

3) accurate and, where necessary, for purposes of personal data processing, kept up to date; inaccurate or incomplete data must be rectified, supplemented, erased or their further processing must be suspended;

4) identical, adequate and not excessive in relation to the purposes for which they are collected and further processed;

5) kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the data were collected and processed.

6) processed in compliance with the clear and transparent requirements for personal data processing set forth in this Law and other laws regulating relevant activities.

2. Personal data collected for other purposes may be processed for statistical, historical or scientific research purposes only in the cases laid down by laws, provided that adequate data protection measures are laid down by laws.

Article 4. Storage and Destruction of Personal Data

Personal data shall not be stored longer than it is necessary for data processing purposes. Personal data must be destroyed when they are no more needed for their processing purposes, with the exception of data which must be transferred to state archives in the cases laid down by laws.

Article 5. Criteria for the Lawful Processing of Personal Data

1. Personal data may be processed if:

1) the data subject has given his consent;

2) a contract to which the data subject is party is being concluded or performed;

3) it is a legal obligation of the data controller under laws to process personal data;

4) processing is necessary in order to protect vital interests of the data subject;

5) processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data are disclosed;

6) processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless such interests are overridden by interests of the data subject.

2. It shall be prohibited to process special categories of personal data, except in the following cases:

1) the data subject has given his consent;

2) such processing is necessary for the purposes of employment or civil service while exercising rights and fulfilling obligations of the data controller in the field of labour law in the cases laid down in laws;

3) it is necessary to protect vital interests of the data subject or of any other person, where the data subject is unable to give his consent due to a physical disability or legal incapacity;

4) processing of personal data is carried out for political, philosophical, religious purposes or purposes concerning the trade-unions by a foundation, association or any other non-profit organisation, as part of its activities, on condition that the personal data processed concern solely the members of such organisation or to other persons who regularly participate in such organisation in connection with its purposes. Such personal data may not be disclosed to a third party without the data subject's consent;

5) the personal data have been made public by the data subject;

6) the data are necessary, in the cases laid down in laws, to prevent and investigate criminal or other unlawful acts;

7) the data are necessary for a court hearing;

8) it is a legal obligation of the data controller under laws to process such data.

3. Data on a person's health may also be processed for the purposes and in the procedure laid down in Article 10 of this Law and other laws regulating health care.

4. The personal data related to a person's record of conviction, criminal acts or security measures may be processed, for crime prevention, investigation purposes and in other cases laid down by laws, only by a state institution or agency in the manner laid down in laws. Other natural or legal persons may process such data in the cases laid down by laws provided that appropriate measures laid down in laws and other legal acts for the protection of legitimate

interests of the data subject have been adequately implemented. Detailed data about previous convictions may be processed only according to the procedure laid by the Law on State Registers.

Article 6. Disclosure of Personal Data

In the cases laid down in this Law, personal data shall be disclosed under a personal data disclosure contract between the data controller and the data recipient in the case of a multiple disclosure or in response to a request of the data recipient in the case of a single disclosure. The contract must specify the purpose for which personal data will be used, the legal basis for disclosure and receipt, the conditions, the procedure of use and the extent of personal data that is disclosed. The request must specify the purpose for which personal data will be used, the legal basis for disclosure and receipt and the extent of personal data requested. Where personal data are managed by automatic means and appropriate measures ensuring data security are applied, in disclosing personal data under a personal data disclosure contract between the data controller and the data recipient priority must be given to disclosure of the data by automatic means, and when disclosing personal data at the request of the data recipient – to disclosure of data by means of electronic communications.

Article 7. Use of a Personal Identification Number

1. A personal identification number shall be a unique sequence of digits. A personal identification number shall be assigned to a person in accordance with the procedure laid down in the Law on Residents' Register.

2. It shall be permitted to use a personal identification number when processing personal data only with the consent of the data subject, except in cases specified in paragraphs 4 and 5 of this Article, when the use of the personal identification number shall be prohibited.

3. A personal identification number may be used without the consent of the data subject only if:

1) such a right is laid down in this Law and other laws;

2) a scientific or statistical research is being carried out in the cases laid down in Articles 12 and 13 of this Law;

3) it is processed in state or departmental registers, provided that they have been officially set up in accordance with the procedure laid down in the Law on State Registers, and in information systems, provided that they have been set up in accordance with the procedure laid down in legal acts;

4) it is processed by legal persons involved in activities related to granting of loans and

recovery of debts, insurance or financial leasing, health care and social insurance as well as in the activities of other institutions providing and administrating social care, educational establishments, research and higher education institutions. Legal persons specified in this point may use personal identification number only for the purpose for which it has been received and only in these cases where it is necessary for a legitimate and specified purpose of personal data processing;

5) classified data are processed in cases laid down by laws.

4. A personal identification number may not be made public.

5. A personal identification number may not be collected and processed for direct marketing purposes.

Article 8. Processing of Personal Data and Adjustment of the Freedom of Provision of Information to the Public

The processing of personal data by the media for the purpose of providing information to the public, artistic and literary expression shall be supervised by the Inspector of Journalist Ethics. The remit thereof shall be laid down by the Law on Provision of Information to the Public. In these cases, only the provisions of Articles 1, 2, 3, 4, 5, 6, 7, 30, 53 and 54 of this Law shall apply to the processing of personal data.

Article 9. Personal Data Processing for the Purposes of Social Insurance and Social Assistance

For the purposes of social insurance and social assistance administrative institutions of the State Social Insurance Fund and legal persons providing or administering social assistance shall exchange personal data without the data subject's consent.

Article 10. Personal Data Processing for the Purposes of Health Care

1. Personal data on a person's health (its state, diagnosis, prognosis, treatment, etc.) may be processed by an authorised health care professional. A person's health shall be subject to professional secrecy under the Civil Code, the laws regulating patients' rights and other legal acts.

2. Personal data processing for scientific medical research purposes shall be carried out in accordance with this and other laws.

3. Personal data on a person's health may be processed by automatic means, also for scientific medical research purposes only subject to giving a notice to the State Data Protection Inspectorate. In this case, the State Data Protection Inspectorate must carry out a prior checking.

Article 11. Personal Data Processing for the Purposes of Elections, Referendum and Citizens' Legislative Initiative

1. Processing of personal data (name, surname, date of birth, personal identification number, address of the place of residence, citizenship, number of the identification document) for the purposes of elections, referendum, citizens' legislative initiative, political campaigns and financing of political parties shall be determined by this Law and other laws.

2. Information compiled by the Central Electoral Commission on the basis of statements and other documents submitted by candidates or their representatives and announced on a website, about candidates, votes received by the candidates, lists of members of electoral or referendum committees, observers, representatives, members of initiative groups and lists of donors of political campaigns may be revised after the announcement of election or referendum results, only for the purposes of correction of language mistakes or when the information on the website differs from the information in the statements and other documents delivered at the time prescribed by legal acts. Personal identification numbers of the candidates and any other persons, their citizenship or numbers of their identification documents, the exact address (street, number of the house, number of the apartment) of their place of residence may not be made public on the website.

Article 12. Personal Data Processing for the Purposes of Scientific Research

1. Personal data may be processed for the purposes of scientific research on condition that the data subject has given his consent. Without the data subject's consent, personal data may be processed for the purposes of scientific research only upon giving a notice to the State Data Protection Inspectorate. In this case, the State Data Protection Inspectorate must carry out a prior checking.

2. Personal data which have even used for the purposes of scientific research must be altered immediately in a manner which makes it impossible to identify the data subject.

3. The personal data collected and stored for the purposes of scientific research may not be used for any other purposes.

4. In the cases when the conducted research does not require personal identification data, the data controller shall provide to the data recipient such personal data from which identification of a person is not possible.

5. Research results shall be made public together with the personal data on condition that the data subject has given his consent to have his personal data made public.

Article 13. Personal Data Processing for Statistical Purposes

1. The processing of personal data for statistical purposes shall mean the carrying out of statistical surveys and disclosure and storage of their results.

2. The personal data collected for other than statistical purposes may be used in the cases laid down by law for the preparation of official statistical information.

3. The personal data collected for statistical purposes may be disclosed and used for other than statistical purposes in accordance with the procedure and in the cases laid down in the Law on Statistics.

4. The personal data collected for different statistical purposes shall be compared and combined only on condition that the personal data are protected against unlawful use for other than statistical purposes.

5. Special categories of personal data shall be collected for statistical purposes solely in the form which does not permit direct or indirect identification of the data subject, except in the cases laid down by law.

Article 13[1]. Personal Data Processing for the Purposes of a Social and Public Opinion Survey

1. When conducting a social and public opinion survey, personal data may be processed only with the consent of a data subject. The data subject's contact data (address, phone number) may be processed without the data subject's consent until the first direct contact with the data subject, with the aim of contacting him. The data subject shall grant his consent to personal data processing for the purposes of a social and public opinion survey or refuse to grant it in the course of a direct contact with the conductor of the survey or in a written or equivalent form. Where the data subject refuses to grant his consent to personal data processing, such personal data must be immediately destroyed.

2. Only the personal data which are necessary for conducting a social and public opinion survey must be collected for the purposes of the social and public opinion survey; the personal data used for a specific social and public opinion survey must be altered immediately in a manner which makes it impossible to identify the data subject.

3. The use of the personal data collected and processed for the purposes of a social and public opinion survey for other purposes (for advertising, direct marking, commercial activities, etc.) shall be prohibited.

Article 14. Personal Data Processing for the Purposes of Direct Marketing

1. Personal data may be processed for the purposes of direct marketing only after the data

subject gives his consent.

2. Personal data may be processed for the purposes of direct marketing if a period for the storage of personal data is set when collecting such data.

3. The data controller must provide a clear, free-of-charge and easily realisable possibility for the data subject to give or refuse giving his consent for the processing of his personal data for the purposes of direct marketing.

4. The data controller who, while rendering services or selling goods in accordance with the procedure and conditions set by this Law, receives contact information (name, surname and address) from the data subjects being his customers may only use this data without a separate data subject's consent for the marketing of his own goods or services of a similar nature provided that the customers have been given a clear, free-of-charge and easily realisable possibility not to give their consent or refuse giving their consent for the use of this data for the above-mentioned purposes at the time of collection of the data and, if initially the customer has not objected against such use of the data, at the time of each offer.

Article 15. Personal Data Processing in the Areas of Electronic Communications and Cyber Security

The processing of personal data in the areas of electronic communications and cyber security shall be governed by the Law on Electronic Communications, the Law on Cyber Security and this Law.

Article 15^{1}. Personal Data Processing in the Framework of Police and Judicial Cooperation in Criminal Matters as Provided for in Title V of Part Three of the Treaty on the Functioning of the European Union

In the framework of police and judicial co-operation in criminal matters as provided for in Title V of Part Three of the Treaty on the Functioning of the European Union, personal data shall be processed in compliance with the Law on Legal Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters and this Law.

CHAPTER THREE
VIDEO SURVEILLANCE

Article 16. Conditions of Video Surveillance

Video surveillance may be used for the purpose of ensuring public safety, public order and protecting person's life, health, property and other rights and freedoms of persons but only in

these cases when other means or measures are insufficient and/or inadequate for the achievement of the above-mentioned purposes unless they are overridden by the interests of the data subject.

Article 17. Video Surveillance in the Workplace

Video surveillance in the workplace may be used only when because of the specifics of the work it is necessary to ensure security of persons, property or the public and in other cases when other means or measures are insufficient and/or inadequate for the achievement of the above-mentioned purposes.

Article 18. Requirements for Video Surveillance

1. The processing of video data must be specified in a written document approved by the data controller and indicating the purpose and the extent of video surveillance, the period of retention of the video data, conditions of access to the video data being processed, conditions of and procedure for destroying these data and other requirements for the lawful processing of the video data.

2. The data controller shall ensure that video data are processed only by persons who have been authorised by the data controller and who must be instructed on legal acts regulating legal protection of personal data and committed to abide by them against signature.

Article 19. Installation of Video Surveillance Devices

1. Taking into account the specified purpose of video surveillance, video surveillance devices must be installed in such a manner so as to ensure that:

1) video surveillance does not cover a larger part of the premises or territory than it is necessary;

2) video data are collected only to such an extent that is necessary.

2. It shall be prohibited to install and operate installed video surveillance devices in such a manner that the area of surveillance covers residential premises and/or the adjacent private territory or entrance thereto, except for the cases specified by laws. In common-use premises, video surveillance devices may be installed by a decision of the majority of co-owners.

3. It shall be prohibited to use video surveillance in premises where the data subject reasonably expects absolute protection of privacy and where such surveillance would undermine human dignity (e.g., toilets, changing-rooms, etc.).

Article 20. Notification of the Data Subject of Video Surveillance

1. The data controller shall ensure that the following information is clearly and properly

provided prior to the entrance to the premises or territory in which video surveillance is used:

1) information about the use of video surveillance therein;

2) the name and company's number of the data controller, where the data controller is a legal person, the name and surname of the data controller, where the data controller is a natural person, the contact information thereof (address or phone number).

2. The data controller may provide also other additional information relevant for ensuring the lawful processing of personal data without infringing the data subject's rights (e.g., the purpose of video surveillance).

3. If video surveillance is used in the workplace and in the data controller's premises or territories in which the data controller's personnel work, the personnel must be notified of such processing of their image data in writing according to the procedure laid down in Article 24(1) of this Law.

CHAPTER FOUR
PROCESSING OF PERSONAL DATA ON EVALUATION OF SOLVENCY AND DEBT MANAGEMENT

Article 21. Personal Data Processing for the Purpose of Evaluating a Person's Solvency and Managing His Debt

1. The data controller shall have the right to process and disclose to third parties having legitimate interests the data, including personal identification numbers, of the data subjects who have failed to fulfil, in a timely and proper manner, their financial and/or property obligations to the data controller (hereinafter: 'debtors') for the purpose of evaluating their solvency and managing their debt, provided that data protection requirements set out in this Law and other legal acts are duly complied with.

2. The data controller shall have the right to disclose debtors' data, including personal identification numbers, to other data controllers who process consolidated debtor files (hereinafter: 'consolidated debtor files'). The data controller may process consolidated debtor files for the purpose of disclosing such data to third parties having legitimate interests so that they could evaluate the solvency of the data subject and manage his debt only if he has notified, according to the procedure laid down in Article 33 of this Law, the State Data Protection Inspectorate, which must carry out a prior checking.

3. The data controller may disclose debtors' data on condition that he has sent a written reminder by post or by means of electronic communications to the data subject about a default on obligations and where, within 30 calendar days from sending/submitting the reminder:

1) the debt is not settled and/or the deadline for the repayment is not extended; or

2) the data subject does not contest the debt on compelling grounds.

4. The data controller may not process special categories of personal data.

5. Consolidated debtor files may not be combined with personal data from other personal data files which have been compiled and are processed for purposes other than evaluation of solvency and debt management.

6. The data controller processing consolidated debtor files must, upon receiving debtors' data from the data controller referred to in paragraph 2 of this Article, provide each data subject with the following information (unless the data subject already has such information at his disposal):

1) his (the data controller's) and his representative's, if any, name, company's number and the address of the registered office;

2) the purposes of processing of the data subject's personal data;

3) the sources and the type of the data subject's data which have been collected, the recipient and the purposes for which the data are disclosed, the data subject's right of access to his personal data and the right to request rectification of incorrect, inaccurate and incomplete personal data.

7. The data about the default of data subject on a timely and proper fulfilment of his financial and/or property obligations may not be processed for a period longer than ten years from the date of settlement of the debt. Where the data subject repays his debt, data controllers must ensure that during the processing data about the data subject's default on timely and proper fulfilment of his financial and/or property obligations the following information is specified:

1) the fact of settlement of the debt by the data subject;

2) the date of the debt settlement.

Article 22. Processing of Personal Data on the Rendered Financial Services Related to Risk Acceptance or Creditworthiness for the Purpose of Evaluation of a Person's Solvency and Financial Risk and Debt Management

1. Credit institutions and financial undertakings providing financial services related to risk acceptance or credit rating (hereinafter: 'financial services') (hereinafter: 'financial institutions') shall have the right to process and to receive from each other the personal data (name, surname, personal identification number (in the absence of the personal identification number – data of a personal document), address, phone number, the type and the amount of the requested financial and/or property obligations which have been granted or denied, the type, the amount and terms of fulfilment of existing financial and/or property obligations, data on the fulfilment of these

obligations as well as data on previous financial and/or property obligations and their fulfilment, including data of data subjects contained in consolidated debtor files, also data on the income of the data subjects, the type and source of such income, data on the assets, marital status, position/occupation and education of the data subjects) of the data subjects to whom the credit institutions and financial undertakings have rendered or intend to render financial services and of the data subjects providing security for obligations to the above-mentioned institutions and undertakings, for the purposes of evaluation of a person's solvency and financial risk as well as debt management on the condition that the data subjects have given their consent.

2. Where the data subject gives his consent, the data referred to in paragraph 1 of this Article may be processed for the purposes of evaluation of a person's solvency and financial risk and debt management and be regularly updated in consolidated files of financial risk data (hereinafter: 'consolidated financial risk files') under the data provision arrangements concluded with financial institutions. Financial institutions may act as controllers of consolidated financial risk files only upon notifying, in accordance with the procedure laid down by Article 33 of this Law, the State Data Protection Inspectorate, which must carry out a prior checking.

3. Financial institutions may obtain personal data on the conditions and within the scope of paragraph 1 of this Article only when the data subject:

1) applies to these institutions for rendering of financial services or provision of security for fulfilment of financial and/or property obligations, and/or;

2) has been rendered financial services by these institutions or has provided security for fulfilment of financial and/or property obligations and it is necessary to evaluate the existence of the risk for the proper fulfilment of the undertaken obligations.

4. Financial institutions shall ensure that the received data of data subjects are not:

1) processed for the purposes incompatible with the purposes determined before collecting the personal data;

2) stored for a period longer than 12 months, if a decision refusing to render a financial service is taken.

5. Financial institutions shall ensure that data on the financial services rendered by them are not stored for a period longer than ten years from the date of rendering these services and fulfilment of obligations, unless laws or legal acts adopted on their basis establish otherwise.

6. All personal data contained in consolidated financial risk files may be provided only to financial institutions. Other persons rendering services related to the acceptance of financial risk for the purposes of evaluation of a person's solvency and financial risk and debt management from consolidated financial risk files shall be disclosed only the following generalised data: a person's name, surname, personal identification number (in the absence of the personal

identification number – data of a personal document) and the person's credit rating.

7. It shall be prohibited to disclose personal data and a person's credit rating from consolidated financial risk files for purposes other than evaluation of the person's solvency and financial risk and debt management.

8. The data subject shall have the right to give to the controller of a consolidated financial risk file his/its opinion concerning determination of a person's credit rating in accordance with the procedure laid down by Article 28 of this Law.

CHAPTER FIVE
RIGHTS OF THE DATA SUBJECT

Article 23. Rights of the Data Subject

1. The data subject shall, in accordance with the procedure laid down in this Law, have the right:

1) to know (be informed) about the processing of his personal data;

2) to have an access to his personal data and to be informed of how they are processed;

3) to request rectification or destruction of his personal data or suspension of further processing of his personal data, with the exception of storage, where the data are processed in violation of the provisions of this Law and other laws;

4) to object against the processing of his personal data.

2. The data controller must provide the data subject with the conditions for exercising the rights laid down in this Article, with the exception of cases laid down in laws when it is necessary to ensure:

1) security or defence of the State;

2) public order and prevention, investigation, detection or prosecution of criminal offences;

3) important economic or financial interests of the State;

4) prevention, investigation and detection of violations of official or professional ethics;

5) protection of the rights and freedoms of the data subject or other persons.

3. The data controller must justify a refusal to grant the request of the data subject to exercise the rights granted to the data subject by this Law. Having received a request from the data subject, the data controller must reply him within 30 calendar days from the date of data subject's application. Where the request of the data subject is submitted in writing, the data controller's reply must also be executed in writing.

4. The data subject may appeal against acts/omissions of the data controller to the State Data Protection Inspectorate within three months from the receipt of a reply of the data controller

or within three months from the expiry of a time limit for providing a reply as referred to in paragraph 3 of this Article. The acts/omissions of the State Data Protection Inspectorate may be appealed against to court in accordance with the procedure laid down by law.

Article 24. Provision of the Data Subject with Information about the Processing of Data Related Thereto

1. The data controller must provide the data subject whose personal data he/it collects directly from the latter with the following information, except where the data subject already has such information at his disposal:

1) the identity and permanent place of residence of himself (the data controller) and his representative, if any (where the data controller or his representative is a natural person), or indicate the name, company's number and address of the registered office (where the data controller or its representative is a legal person);

2) the purposes of processing of the data subject's personal data;

3) other additional information (the recipient and the purposes of disclosure of the data subject's personal data; the personal data which the data subject must provide and the consequences of his failure to provide the data, the right of the data subject to have access to his personal data and the right to request for rectification of incorrect, incomplete and inaccurate personal data) to the extent that is necessary for ensuring fair processing of personal data without infringing upon the data subject's rights.

2. Where the data controller obtains personal data not from a data subject, he must inform the data subject thereof before commencing the processing of personal data or, if he intends to disclose the data to third parties, he must inform the data subject thereof at the latest when the data are first disclosed, except in the cases where laws or other legal acts determine a procedure for collecting or disclosing such data and data recipients. In such cases, the data controller must provide the data subject with the following information, except where the data subject already has it at his disposal:

1) the identity and permanent place of residence of himself (the data controller) and his representative, if any (where the data controller or his representative is a natural person), or indicate the name, company's number and address of the registered office (where the data controller or its representative is a legal person);

2) the purposes of the processing or the intended processing of the data subject's personal data;

3) other additional information (the sources and the type of the data subject's personal data which are or will be collected; the recipient of the data subject's personal data and the purposes

of the disclosure; the date subject's right to have access to his personal data and his right to request rectification of incorrect, incomplete and inaccurate personal data to the extent necessary to ensure fair processing of personal data without infringing upon the rights of data subjects.

3. When the data controller collects or intends to collect personal data from the data subject and processes or intends to process the data for the purposes of direct marketing, before disclosing data subject's data he must inform the data subject about the recipient of his personal data and the purposes for which his personal data will be disclosed.

4. Paragraph 2 of this Article shall not apply to the processing of personal data for the statistical, historical or scientific research purposes, where the disclosure of such information proves impossible or involves a disproportionate effort (owing to a large number of data recipients, the outdated character of the data and excessively large expenses) or where the procedure for collecting and disclosing of data is laid down by law, also to the processing of the data subject's contact data (address, phone number) for the purposes of a social and public opinion survey until the first direct contact with the data subject. In such cases, the data controller must notify the State Data Protection Inspectorate thereof in accordance with the procedure laid down in Article 33 of this Law. The State Data Protection Inspectorate must carry out a prior checking.

Article 25. Right of the Data Subject to Access His Personal Data

1. The data subject shall have the right, upon presenting to the data controller or the data processor a document certifying his identity or upon confirming his identity in accordance with the procedure laid down by legal acts or by means of electronic communications which permit a person's identification, to obtain information on the sources and type of his personal data which have been collected, the purpose of their processing and the data recipients to whom the data are disclosed or were disclosed at least during the past year.

2. Having received an enquiry from a data subject concerning the processing of his personal data, the data controller must reply to the data subject whether the personal data relating thereto are processed, and disclose to the data subject the requested data no later than within 30 calendar days from the receipt of the data subject's enquiry. At the request of the data subject, such data must be disclosed in writing. The data controller shall disclose such data to the data subject free of charge once per calendar year. When such data are disclosed for a fee, the amount of the fee may not exceed the cost of disclosure of the data. The procedure governing the fee for disclosure of data shall be determined by the Government.

Article 26. Right of the Data Subject to Request Rectification, Destruction or

Suspension of Further Processing of His Personal Data

1. Where the data subject, after familiarising with his personal data, finds that his personal data are incorrect, incomplete or inaccurate and applies to the data controller, the latter must check the personal data concerned without delay and, at a written request of the data subject submitted in person, by post or by means of electronic communications, rectify the incorrect, incomplete and inaccurate personal data and/or suspend the processing of such personal data, except storage, without delay.

2. Where the data subject, after familiarising with his personal data, finds that his personal data are processed unlawfully and unfairly and applies to the data controller, the latter must check without delay and free of charge the lawfulness and fairness of the processing of personal data and, at a written request of the data subject, without delay destroy the personal data collected unlawfully and unfairly or suspend the processing operations of such personal data, except storage.

3. When, at the data subject's request, the processing of his personal data is suspended, the personal data concerned must be stored until they are rectified or destroyed either at the data subject's request or upon expiry of their storage period. Other processing operations of such personal data may be performed solely:

1) for the purpose of giving proof of the existence of circumstances due to which the processing of the data was suspended;

2) where the data subject gives his consent for further processing of his personal data;

3) where the rights or legitimate interests of third parties need to be protected.

4. The data controller must, without delay, notify the data subject of the rectification, destruction of personal data or suspension of the processing of personal data performed or not performed at the data subject's request.

5. Personal data shall be rectified and destroyed or their processing shall be suspended at the data subject's request on the basis of the documents confirming his identity and his personal data.

6. If the data controller questions the accuracy of the personal data provided by the data subject, he must suspend the processing of such data, check and update the data. Such personal data may be used solely for the purpose of checking their accuracy.

7. The data controller must, without delay, inform data recipients of the rectification, destruction or suspension of the processing of the data subject's personal data at the request of the data subject, unless the disclosure of such information proves impossible or involves a disproportionate effort (owing to a large number of data subjects, the period covered by the data, and excessively large expenses). In such a case, the State Data Protection Inspectorate must be

notified without delay.

Article 27. Right of the Data Subject to Object to the Processing of His Personal Data

1. In the cases referred to in Article 5(1)(5) and (6) of this Law, also when data are or are intended to be processed for the purposes of direct marketing, the data controller must inform the data subject about his right to object to the processing of his personal data.

2. In the cases specified in Article 5(1)(5) and (6) of this Law, the data subject shall have the right to object to the processing of his personal data. The data subject shall submit a written notice of objection to the processing of personal data to the data controller in person, by post or by means of electronic communications. Where the objection of the data subject is legally justified, the data controller must, without delay and free of charge, terminate the processing operations of his personal data, except in the cases laid down by laws, and duly notify the data recipients.

3. The data subject shall have the right to object to the processing of his personal data without providing reasons for such objection where the data are or are intended to be processed for the purposes of direct marketing. In such a case, the data controller must, without delay and free of charge, terminate personal data processing operations, except in the cases laid down by laws, and duly notify data recipients.

4. At the data subject's request, the data controller must notify the data subject of termination of or refusal to terminate personal data processing operations.

Article 28. Evaluation of Personal Aspects by Automatic Means

1. No decision may be taken in respect of the data subject's personal aspects (his creditworthiness, reliability, ability to work, etc.) where such aspects have been evaluated solely by automatic means, where such a decision might produce legal effects concerning the data subject or affect him otherwise, with the exception of the following cases:

1) the decision is taken in accordance with the procedure laid down by laws, where the laws provide measures for the protection of the data subject's legitimate interests;

2) the decision is taken when entering into or performing a contract, provided that the data subject's request for the entry into or performance of the contract has been satisfied;

3) the decision is taken when entering into or performing a contract, provided that there are suitable measures to safeguard the data subject's legitimate interests, for example, a procedure allowing the data subject to express his opinion is established.

2. Before commencing an evaluation of personal aspects of the data subject by automatic means, the data controller must provide the data subject with access to the evaluation criteria and

principles established by the data controller.

3. Where, following an evaluation of the data subject's personal aspects by the data controller by automatic means, the data subject disagrees with the evaluation, he shall have the right to express his opinion about the evaluation of his personal aspects. The data controller must take the data subject's opinion into account and, if necessary, repeat the evaluation by means other than automatic means.

Article 29. Assistance to the Data Subject in Exercising His Right of Access to His Personal Data

1. The State Data Protection Inspectorate shall assist the data subject in exercising his right of access to his personal data.

2. Upon submitting a written request and presenting a document confirming his identity to the State Data Protection Inspectorate or upon submitting a request by means of electronic communications and confirming his identity in accordance with the procedure laid down by the State Data Protection Inspectorate, the data subject shall have the right to request the supervisory authority to collect his personal data or information on the processing of his personal data from registered data controllers and to provide him with access to the collected data or information. A reply to this request must be provided in person, by post, by automatic means or by means of electronic communications not later than within 30 calendar days from submission of the request and confirmation of the person's identity.

3. When providing the data subject with the assistance referred to in paragraph 2 of this Article, the State Data Protection Inspectorate shall not have the right to collect the data which are specified in the Law on State Secrets and Official Secrets and which constitute classified information.

4. A state fee in the amount determined by the Government shall be levied for the assistance to the data subject referred to in paragraph 2 of this Article.

5. Having received from the State Data Protection Inspectorate an enquiry regarding the exercise of the right of a particular data subject to have access to his personal data, the data controllers registered in the State Register of Personal Data Controllers must reply to the State Data Protection Inspectorate within 15 calendar days in accordance with the procedure established by the latter (specifying the personal data requested by the data subject or providing information regarding the processing of his personal data, or indicating that the data of the data subject are not processed).

6. Data controllers must ensure the security, confidentiality, integrity and accessibility of the data subjects' data received from and disclosed to the State Data Protection Inspectorate.

CHAPTER SIX
SECURITY OF DATA

Article 30. Security of Data

1. The data controller and the data processor must implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The mentioned measures must ensure a level of security appropriate in respect of the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (the personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.).

2. The State Data Protection Inspectorate shall lay down general requirements for organisational and technical data security measures.

3. The data controller shall process personal data himself/itself and/or authorise the data processor. Where the data controller authorises the data processor to process personal data, he/it must choose a data processor providing guarantees in respect of adequate technical and organisational data protection measures and ensuring compliance with those measures.

4. When authorising the data processor to process personal data, the data controller shall establish that personal data must be processed only in accordance with the data controller's instructions.

5. The relations between the data controller and the data processor who is not the data controller must be regulated by a written contract, except where such relations are regulated by laws or other legal acts.

6. Employees of the data controller, the data processor and their representatives who process personal data must keep confidentiality of personal data, unless such personal data are intended for public disclosure. This obligation shall continue after leaving civil service, transfer to another position or expiry of employment or contractual relations.

7. Printed written information notifications about the services rendered to data subjects (natural persons), the obligations of data subjects (natural persons), performance of contracts with data subjects (natural persons), accounts, salary slips issued by the employer to the employee, individual proposals of a commercial character for data subjects (natural persons) the contents of which contains personal data of data subjects, including, but not limited to, the data concerning a person's name and surname, place of residence, taxes paid or not paid, fiscal code or tax reference number, number of settlement book, sent or disclosed to the data subjects

(natural persons) must be disclosed in a closed form containing only the information necessary for postal services, and the contents of the notifications may be visible only to the data subject (natural person) who is the addressee of the notification or, with his consent, to a third person when opening or unpacking the disclosed notification. These provisions shall not apply where the notifications concerned are delivered to data subjects of personal data (natural persons) in person and confidentially.

8. Data controllers and the persons at whose request the written information notifications referred to in paragraph 7 of this Article are delivered shall be responsible for proper implementation of the requirements indicated in paragraph 7 of this Article.

CHAPTER SEVEN
REGISTRATION OF DATA CONTROLLERS

Article 31. Notification of Data Processing

Personal data may be processed by automatic means only when the data controller or his/its representative (pursuant to Article 1(3)(3) of this Law) notifies the State Data Protection Inspectorate in accordance with the procedure established by the Government, except when personal data are processed:

1) for the purposes of internal administration;

2) for political, philosophical, religious or trade union-related purposes by a foundation, association or any other non-profit organisation on condition that the personal data processed relate solely to the members of such organisation or to other persons who regularly participate in its activities in connection with the purposes of such organisation;

3) in the cases laid down in Article 8 of this Law;

4) in accordance with the procedure laid down in the Law on State Secrets and Official Secrets.

Article 32. Person or Unit Responsible for Data Protection

1. The data controller shall have the right to appoint/designate a person or unit to be responsible for data protection.

2. A person or unit responsible for data protection shall:

1) make public the actions of personal data processing carried out by the data controller in accordance with the procedure established by the Government;

2) supervise as to whether personal data are processed in compliance with the provisions of this Law and other legal acts regulating data protection;

3) initiate the preparation of notifications to the State Data Protection Inspectorate regarding the existence of the circumstances indicated in Article 33(1) of this Law;

4) monitor the processing of personal data carried out by the data controller's employees;

5) present proposals, findings to the data controller regarding determination of data protection and data processing measures and supervise the implementation and use of these measures;

6) undertake, without delay, measures to eliminate any violations in the processing of personal data;

7) instruct the employees authorised to process personal data on the provisions of this Law and other legal acts regulating personal data protection;

8) initiate preparation of applications to the State Data Protection Inspectorate on the issues of the processing and protection of personal data;

9) assist data subjects in exercising their rights;

10) notify the State Data Protection Inspectorate in writing upon establishing that the data controller processes personal data in violation of the provisions of this Law and other legal acts regulating data protection and refuses to rectify these violations.

3. The data controller must provide a person or unit responsible for data protection with complete information about the planned data processing and the intended use of automatic means of data processing and lay down a reasonable time limit for presenting a conclusion on the intended personal data processing.

4. The data controller must enable a person or unit responsible for data protection to independently perform his/its functions as specified in this Article.

5. The data controller must, within 30 calendar days, notify the State Data Protection Inspectorate of appointment/designation or removal of a person or unit responsible for data protection.

Article 33. Prior Checking

1. The State Data Protection Inspectorate shall carry out prior checking in the following cases:

1) where the data controller intends to process special categories of personal data by automatic means, except where the processing is carried out for the purposes of internal administration or in the cases laid down in Article 5(2)(6) and (7) of this Law;

2) where the data controller intends to process public data files by automatic means, unless laws and other legal acts lay down a procedure for the disclosure of data;

3) where the data controller of state or departmental registers or information systems of

state and municipal institutions intends to authorise the data processor to process personal data, except in the cases where laws and other legal acts establish the right of the data controller to authorise a particular data processor to process personal data or where the data processor is a legal person established by the data controller;

4) in the cases laid down in Article 10(3), Article 12(1), Article 21(2), Article 22(2), Article 24(4) of this Law and in the case specified by other laws.

2. The data controller must notify the State Data Protection Inspectorate, in accordance with the procedure established by the State Data Protection Inspectorate, of the cases referred to in paragraph 1 of this Article. Such data processing operations may be carried out only upon obtaining an authorisation of the State Data Protection Inspectorate. The State Data Protection Inspectorate must carry out prior checking in accordance with the procedure established by the State Data Protection Inspectorate and grant or refuse to grant an authorisation to the data controller to carry out personal data processing within two months from the receipt of the notification, except in the cases where due to the complexity of the circumstances referred to in the notification, the extent of information or other relevant circumstances, the period of examination of the notification must be extended. In such cases, the period of examination of the notification shall be extended, but not longer than for one month, subject to giving a notice thereof to the data controller. A decision of the State Data Protection Inspectorate to refuse an authorisation to the data controller to carry out personal data processing operations may be appealed against in accordance with the procedure laid down by laws.

Article 34. Registration of Data Controllers

1. Data controllers shall be registered in the State Register of Personal Data Controllers.

2. The State Register of Personal Data Controllers shall be administered by the State Data Protection Inspectorate.

CHAPTER EIGHT
TRANSFER OF PERSONAL DATA TO DATA RECIPIENTS IN FOREIGN COUNTRIES

Article 35. Transfer of Personal Data to Data Recipients in Foreign Countries

1. Personal data shall be transferred to data recipients in the Member States of the European Union or other countries of the European Economic Area under the same conditions and in accordance with the same procedure as to data recipients in the Republic of Lithuania.

2. Transfer of personal data to data recipients in third countries shall be subject to

obtaining an authorisation of the State Data Protection Inspectorate, except in the cases referred to in paragraph 5 of this Article.

3. The State Data Protection Inspectorate shall grant or refuse to grant an authorisation for transfer of personal data to third countries not later than within two months from the receipt of an application for the granting of the authorisation by the data controller. An authorisation shall be granted provided that there is an adequate level of legal protection of personal data in these countries. The level of legal protection of personal data shall be assessed by considering all circumstances related to transfer of data particularly the laws and other legal acts or acts prepared by the data controller on legal protection of personal data in force in the third country of destination, the nature of the data to be transferred, methods, purposes and duration of the data processing and safeguards applicable in the country concerned.

4. The State Data Protection Inspectorate may grant an authorisation for transfer of personal data to a third country which cannot guarantee an adequate level of legal protection of personal data on condition that the data controller has established adequate data protection safeguards for the protection of a person's right to private life and the protection and exercise of other rights of the data subject. Such safeguards must be stipulated in a contract on the transfer of personal data to a third country or in another document drawn up in writing.

5. Without an authorisation of the State Data Protection Inspectorate, personal data shall be transferred to a third country or to an international law enforcement organisation only if:

1) the data subject has given his consent for the transfer of his personal data;

2) the transfer of personal data is necessary for the conclusion or performance of a contract between the data controller and a third party in the interests of the data subject;

3) the transfer of personal data is necessary for the performance of a contract between the data controller and the data subject or for the implementation of pre-contractual measures to be taken in response to the data subject's request;

4) the transfer of personal data is necessary (or required by laws) on grounds of overriding public interest or for the purpose of hearing of a case in court;

5) the transfer is necessary for the protection of vital interests of the data subject;

6) the transfer is necessary for the prevention or investigation of criminal acts;

7) personal data are transferred from a public data file in accordance with the procedure laid down by laws and other legal acts.

CHAPTER NINE
SHAPING OF STATE POLICY IN THE FIELD OF PERSONAL DATA PROTECTION AND SUPERVISION OF IMPLEMENTATION OF THIS LAW

Article 35[1]. Functions of the Ministry of Justice in the Field of Protection of Personal Data

The Ministry of Justice shall:

1) shape state policy in the field of personal data protection;

2) shape Lithuania's policy in the field of the EU's personal data protection;

3) draft laws regulating the protection of personal data;

4) perform functions in the field of personal data protection as prescribed by other legal acts.

Article 36. Supervisory Authority and Legal Status Thereof

1. The implementation of this Law, with the exception of Article 8 and Article 35[1], shall be supervised and monitored by the State Data Protection Inspectorate. The State Data Protection Inspectorate shall be a Government body financed from the state budget. The administrative structure thereof shall be approved by the Government or the approval thereof shall be delegated to the head of the State Data Protection Inspectorate. The regulations of the State Data Protection Inspectorate shall be approved by the Government.

2. The State Data Protection Inspectorate shall be a public legal person with its own bank account and a seal with the coat of arms of the Republic of Lithuania and its name.

3. The key objectives of activities of the State Data Protection Inspectorate shall be supervision of data controllers' activities when processing personal data, monitoring of the lawfulness of personal data processing, prevention of violations in data processing and ensuring of the protection of rights of the data subject.

4. The State Data Protection Inspectorate shall not have the right to monitor the processing of personal data which is carried out by courts when administering justice.

Article 37. Legal Basis and Principles of Activities of the State Data Protection Inspectorate

1. In its activities, the State Data Protection Inspectorate shall be guided by the Constitution of the Republic of Lithuania, international treaties of the Republic of Lithuania, this Law and other laws and legal acts.

2. Activities of the State Data Protection Inspectorate shall be based on the principles of

lawfulness, impartiality, publicity and professionalism in the discharge of its functions. The State Data Protection Inspectorate shall be independent as regards discharge of its functions established by this Law and taking of the decisions related to the discharge of the functions established by this Law. Its rights may be restricted only by laws.

3. State and municipal institutions and agencies, members of the Seimas, other officials, political parties, public organisations, other legal and natural persons shall not have the right to exert any kind of political, economic, psychological or social pressure or other unlawful influence on the Director of the State Data Protection Inspectorate, civil servants and employees working under employment contracts. Interference with activities of the State Data Protection Inspectorate shall entail liability established by laws.

Article 38. Status of the Head of the State Data Protection Inspectorate

1. The Sate Data Protection Inspectorate shall be headed by the Director of the State Data Protection Inspectorate. He shall be the manager of state budget appropriations.

2. The Director of the State Data Protection Inspectorate shall be a civil servant, the head of the institution, recruited for a term of office of five years and dismissed by the Government in accordance with the procedure established by the Law on the Government. The Director of the State Data Protection Inspectorate shall be accountable to the Government and the Minister of Justice. A person may be appointed to the position of the Director of the State Data Protection Inspectorate for not more than two successive terms of office.

3. The Director of the State Data Protection Inspectorate must suspend his membership in a political party for the duration of his term of office.

Article 39. Deputies of the Director of the State Data Protection Inspectorate

1. The Director of the State Data Protection Inspectorate shall have deputies.

2. Deputy Directors shall be recruited by the Director of the State Data Protection Inspectorate in accordance with the procedure established by the Law on Civil Service.

3. In the absence of the Director of the State Data Protection Inspectorate, he shall be substituted by one of his deputies, who shall temporarily discharge his functions.

Article 40. Functions of the State Data Protection Inspectorate

The State Data Protection Inspectorate shall:

1) administer the State Register of Personal Data Controllers, make its data public and supervise the activities of data controllers related to the processing of personal data;

2) examine requests of persons in accordance with the procedure laid down in the Law on

Public Administration;

3) in accordance with the procedure laid down by this Law, examine complaints and reports by persons (hereinafter: 'complaints'), check the lawfulness of personal data processing based thereon and take decisions concerning violations in personal data processing;

4) in accordance with the procedure laid down by the Director of the State Data Protection Inspectorate, check the lawfulness of personal data processing and take decisions concerning violations in personal data processing;

5) grant authorisations to data controllers for the transfer of personal data to data recipients in third countries;

6) draw up and publish annual reports on its activities;

7) consult data subjects, data controllers and data processors, other persons regarding the protection of personal data and privacy, also draw up methodological recommendations on the protection of personal data and publish them on the Internet;

8) in accordance with the procedure laid down by laws, provide assistance to data subjects residing abroad;

9) in the cases laid down by laws, provide other states with information about legal acts of the Republic of Lithuania regulating data protection and the practice of their administration;

10) in the cases laid down by this Law and other laws, carry out a prior checking and submit conclusions to the data controller on the intended data processing;

11) co-operate with foreign institutions in charge of the protection of personal data, European Union institutions, agencies and international organisations and take part in their activities;

12) participate in the shaping of state policy in the field of protection of personal data and implement it, also implement Lithuania's policy in the field of the EU's personal data protection and provisions of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);

13) participate in the drafting of laws, draft other legal acts regulating the protection of personal data, co-ordinate draft legal acts and submit proposals to the Seimas, the Government, other state and municipal institutions and agencies regarding the drafting, amendment and repealing of laws or other legal acts, provided that their provisions are related to the issues falling within the remit of the State Data Protection Inspectorate;

14) submit proposals to the Ministry of Justice regarding the shaping of state policy in the field of personal data protection and the shaping of Lithuania's policy in the field of the EU's personal data protection;

15) assess the personal data processing rules submitted by data controllers;

16) perform other functions laid down by this Law and other legal acts.

Article 41. Rights of the State Data Protection Inspectorate

The State Data Protection Inspectorate shall have the right:

1) to obtain, free of charge, from state and municipal institutions and agencies, other legal and natural persons all necessary information, copies and transcripts of documents, copies of data, also to access all data and documents necessary for the discharge of its functions of supervision of personal data processing;

2) to obtain access, subject to a prior notice in writing, or without a prior notice where the lawfulness of processing of personal data is to be checked in response to a complaint, to premises of the person being checked (including the premises rented or used on other grounds), or to the territory where the documents and equipment related with the processing of the personal data are kept. Access to the territory, buildings and premises of a legal person (including the buildings and premises rented or used on any other grounds) shall be permitted only during office hours of the legal person being checked upon presenting a certificate of a civil servant. Access to residential premises (including premises leased or used on any other basis) of a natural person being checked, where documents and facilities related with the personal data processing are kept shall be permitted only upon producing a court order authorising entry into the residential premises;

3) to attend sessions of the Seimas and meetings of the Government and other state institutions when their agenda include the issues related to data protection;

4) to invite experts/consultants and set up work groups for the purpose of expert examination of data processing or protection, for the drafting of documents on data protection, also for taking decisions on other issues falling within the remit of the State Data Protection Inspectorate;

5) to issue recommendations and give instructions to the data controller regarding the processing and protection of personal data;

6) to draw up records of administrative offences in accordance with the procedure laid down by laws;

7) to exchange information with personal data supervisory authorities in other countries and with international organisations to the extent necessary for the discharge of their duties;

8) to take part in the hearing of cases in court over violations of the provisions of international and national law on personal data protection;

9) to use photographic, filming and audio recording equipment in collecting evidence in the course of checking of the lawfulness of personal data processing;

10) to exercise other rights laid down by laws and other legal acts.

Article 41[1]. Procedure for Issuing Court Authorisations to Enter Natural Persons' Residential Premises

1. Where the State Data Protection Inspectorate takes a decision on conducting an inspection of a natural person's residential premises (including the premises rented or used on other grounds), a request for the issuance of a court's authorisation to enter the natural person's residential premises shall be submitted to Vilnius Regional Administrative Court.

2. A request for the issuance of a court's authorisation to enter a natural person's residential premises must indicate the name, surname of the natural person to be inspected, the address of the residential premises, the nature of suspected violations.

3. A request for the issuance of a court's authorisation to enter the residential premises of a natural person to be inspected shall be examined by a judge of Vilnius Regional Administrative Court, who shall issue a reasoned order satisfying or rejecting the request.

4. A request for the issuance of a court's authorisation to enter the residential premises of a natural person to be inspected must be examined, and an order must be issued, not later than within 72 hours from the submission of the request.

5. Where the State Data Protection Inspectorate disagrees with an order issued by a judge of Vilnius Regional Administrative Court rejecting a request, it shall have the right, within seven calendar days from passing of the order, to appeal against the order to the Supreme Administrative Court of Lithuania.

6. The Supreme Administrative Court of Lithuania must examine an appeal of the State Data Protection Inspectorate against an order of a judge of Vilnius Regional Administrative Court not later than within seven calendar days from filing of the appeal. A representative of the State Data Protection Inspectorate shall have the right to participate in the hearing of the appeal.

7. A ruling of the Supreme Administrative Court of Lithuania shall be final and not subject to appeal.

CHAPTER TEN
RECEIPT AND INVESTIGATION OF COMPLAINTS

Article 42. Filing of Complaints

1. A person shall have the right to file a complaint with the State Data Protection Inspectorate against acts/omissions of the data controller violating the provisions of this Law.

2. The State Data Protection Inspectorate shall also investigate persons' complaints

forwarded to it by other institutions.

3. Complaints shall generally be filed in writing, including electronic format. The documents lodged by electronic means must bear an advanced electronic signature. Having received an oral complaint or if the State Data Protection Inspectorate has established the existence of elements constituting a violation of this Law from mass media and/or other sources, the State Data Protection Inspectorate may initiate an investigation of its own motion.

4. Oral or written applications by persons requesting to provide explanations, other information or documents and not complaining against acts/omissions by data controllers shall not be considered as complaints.

Article 43. Requirements for a Complaint

1. A complaint shall contain the following information:

1) the addressee – the State Data Protection Inspectorate;

2) the full name and address of the complainant and, at the complainant's request, his telephone number or electronic mail address;

3) the name of the data controller against whom the complaint is filed and the address of the registered office or place of residence thereof, or the address of the place whereat the data are processed;

4) a description of the act/omission complained against, the time and circumstances of commission thereof;

5) the complainant's request to the State Data Protection Inspectorate;

6) the date of drawing up the complaint and the complainant's signature.

2. The evidence available or a description thereof may be attached to a complaint.

3. A failure to keep to the format of a complaint referred to in paragraph 1 of this Article or to provide requisites may not be a basis for refusal to investigate the complaint.

Article 44. Anonymous Complaints

Anonymous complaints shall not be investigated, unless the Director of the State Data Protection Inspectorate decides otherwise.

Article 45. Refusal to Investigate a Complaint

1. The State Data Protection Inspectorate shall take a decision on refusal to investigate a complaint not later than within five working days from the receipt of the complaint and notify the data subject thereof, provided that:

1) the investigation of the circumstances referred to in the complaint falls outside the remit

of the State Data Protection Inspectorate;

2) a complaint on the same issue has already been investigated by the State Data Protection Inspectorate, except for the cases when new circumstances are indicated or new facts are submitted;

3) a complaint on the same issue has been heard or is being heard in court;

4) a procedural decision on the opening of a pre-trial investigation of the subject-matter of the complaint has been taken;

5) the text of the complaint is illegible;

6) more than one year has lapsed since the commission of the violations referred to in the complaint until filing of the complaint.

2. If a decision on refusal to investigate a complaint is taken, reasons for the refusal must be specified.

3. Where the complaint falls outside the remit of the State Data Protection Inspectorate, the State Data Protection Inspectorate shall, within the time limit referred to in paragraph 1 of this Article, forward the complaint to a competent authority and notify the complainant thereof. Where the competent authority is a court, the complaint shall be delivered back to the complainant with the relevant information.

Article 46. Termination of Investigation of Complaints

1. The State Data Protection Inspectorate shall terminate the investigation of a complaint where it receives the complainant's request for the termination of investigation of the complaint. The State Data Protection Inspectorate may initiate an investigation of its own motion.

2. The investigation of a complaint shall be terminated where the circumstances referred to in Article 45(1) of this Law emerge during the investigation or in other cases laid down in this Law.

Article 47. Request for Additional Information from the Complainant

1. A request for the documents and information necessary for the investigation of a complaint from the complainant must be lawful and reasoned.

2. At the request of the State Data Protection Inspectorate, the complainant must deliver documents and information within the time limit specified in the request. The documents and information may be repeatedly requested from the complainant only in exceptional cases and with due justification of the necessity of these documents and information.

3. Where the complainant fails to deliver the documents and information requested by the State Data Protection Inspectorate and an investigation is impossible without these documents

and information, the complaint shall not be investigated.

Article 48. Receipt of Complaints

The receipt of a complaint shall be confirmed by a letter of the State Data Protection Inspectorate. The letter shall indicate the date of receipt of the complaint, the name and telephone number of a civil servant of the State Data Protection Inspectorate investigating the complaint, and the reference number of the complaint. The letter confirming the receipt of the complaint shall be hand-delivered to the complainant or sent to him by post or electronic mail not later than within three working days.

Article 49. Time Limits for Investigation of Complaints

A complaint must be investigated and a reply must be given to the complainant within two months of the receipt of the complaint, unless the investigation requires a longer period owing to the complexity of circumstances indicated in the complaint, plenitude of information or continuous character of actions complained about. In such cases, the period of investigation shall be extended, but not longer than for two months. The entire period of investigation of a complaint may not be longer than four months. The complainant shall be informed of a decision of the State Data Protection Inspectorate to extend the period of investigation of the complaint. Complaints must be investigated within the shortest possible period.

Article 50. Binding Character of Requirements of the State Data Protection Inspectorate

At the request of the State Data Protection Inspectorate, data controllers and other legal and natural persons must immediately deliver information, copies and transcripts of documents, copies of data, also provide access to all data, facilities related to the processing of personal data and documents necessary for the discharge of functions of supervision of personal data processing.

Article 51. Investigation of Complaints and Decisions Adopted by the State Data Protection Inspectorate

1. Upon completion of an investigation, the State Data Protection Inspectorate shall take a reasoned decision:

1) to admit the complaint as justified;

2) to reject the complaint;

3) to dismiss the investigation of the complaint.

2. A decision shall be signed by the Director of the State Data Protection Inspectorate

3. Decisions of the State Data Protection Inspectorate may be appealed against to court in accordance with the procedure laid down by laws.

Article 52. Obligation not to Disclose Secrets or Data Protected by Laws of the Republic of Lithuania

The Director of the State Data Protection Inspectorate, civil servants and other employees of the State Data Protection Inspectorate recruited under employment contracts may not disclose state, official, professional, commercial/industrial, bank and other secrets and personal data protected by laws which they learned in the course of performance of their official duties.

CHAPTER ELEVEN
LIABILITY

Article 53. Liability for Violations of This Law

Persons in violation of this Law shall be liable in accordance with the procedure established by laws.

Article 54. Compensation for Pecuniary and Non-Pecuniary Damage

1. Any person who has sustained damage as a result of unlawful processing of personal data or any other acts/omissions by the data controller, the data processor or other persons violating the provisions of this Law shall be entitled to claim compensation for pecuniary and non-pecuniary damage caused to him/it.

2. The extent of pecuniary and non-pecuniary damage shall be determined by a court.

I promulgate this Law passed by the Seimas of the Republic of Lithuania.

PRESIDENT OF THE REPUBLIC ALGIRDAS BRAZAUSKAS

Annex to
the Republic of Lithuania

LEGAL ACTS OF THE EUROPEAN UNION IMPLEMENTED BY THIS LAW

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 (OJ 2004 special edition, Chapter 13, Volume 15, p. 355).