

**REPUBLIC OF LITHUANIA**

**LAW AMENDING THE LAW ON LEGAL PROTECTION OF PERSONAL DATA**

**11 June 1996 No. I-1374**

**Vilnius**

**(A new version of 1 February 2008, No. X-1444 )**

**Article 1. A New Version of the Law of the Republic of Lithuania on Legal Protection of Personal Data**

The Law of the Republic of Lithuania on Legal Protection of Personal Data shall be amended and set forth to read as follows:

**“REPUBLIC OF LITHUANIA**

**LAW ON LEGAL PROTECTION OF PERSONAL DATA**

**CHAPTER ONE**

**GENERAL PROVISIONS**

**Article 1. Purpose, Objectives and Scope of the Law**

1. The purpose of this Law is protection of an individual's right to private life while 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 the protection of 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 who is established and operating in the territory of Lithuania, as part of its/his activities. Where personal data are processed by a branch office or a representative office of a data controller of Member State of the European Union or another state of the European Economic Area, established and operating in the Republic of Lithuania, such 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 non-member state of the European Union or another state of the European Economic Area (hereinafter – third state), which uses personal data processing means established in the Republic of Lithuania, with the exception of 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 subparagraph, the data controller must have its representative – 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 in the course of his personal activities unrelated to business or profession.

5. When personal data are processed for the purposes of State security or defence, this Law shall apply only where other laws of the Republic of Lithuania do not provide otherwise.

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

7. 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, the data subject, who is identified 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. **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.

11. **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.

12. **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.

13. **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.

14. **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 recourses, and clerical work).

15. **Public data file** shall mean a state register or any other data file which pursuant to laws and other legal acts is intended for the disclosure of information to the public and which may be lawfully used by the public.

16. **Video surveillance** shall mean processing of image data concerning natural person (hereinafter – image data) by using automated video surveillance means (video and photo cameras, etc.) irrespective of whether these data are recorded in a file or not.

## CHAPTER TWO

### PERSONAL DATA PROCESSING

#### **Article 3. Requirements for Personal Data Processing**

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.

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

#### **Article 5. Criteria for 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, in order to prevent and investigate criminal or other illegal activities;

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. The data about 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 pertaining to health care.

4. Personal data relating 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. Forms of 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.

**Article 7. Use of Personal Identification Number**

1. Personal identification number is a unique sequence of digits. Personal identification number is assigned to a person in accordance with the procedure laid down in the Law on the Population Register.

2. It shall be permitted to use 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 personal identification number shall be prohibited.

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

- 1) such a right is laid down in this and other laws;
- 2) a scientific or statistical research is carried out in the cases laid down in Articles 12 and 13 of this Law;
- 3) it is processed in State or institutional 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, science and studies institutions. Legal persons specified in this subparagraph 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. Personal identification number may not be made public.

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

**Article 8. Processing of Personal Data and 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. His competencies shall be laid down in 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 Social Insurance and Social Assistance Purposes**

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 Health Care Purposes**

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, 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 the data may be processed only having notified the State Data Protection Inspectorate. In this case the State Data Protection Inspectorate must carry out prior checking.

#### **Article 11. Personal Data Processing for the Purposes of Elections, Referenda 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, referenda, citizens' legislative initiative, political campaigns and financing of political parties shall be determined by this and other laws.

2. Information compiled by the Central Electoral Committee on the basis of statements and other documents submitted by candidates or their representatives and announced on the Internet 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 Internet 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 Internet website.

### **Article 12. Personal Data Processing for Scientific Research Purposes**

1. Personal data may be processed for scientific research purposes on condition that the data subject has given his consent. Without the data subject's consent, personal data may be processed for scientific research purposes only upon notifying 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 scientific research purposes must be altered immediately in the manner which makes it impossible to identify the data subject.

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

4. In these cases where the conducted researches do not require data identifying a person, 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. Processing of personal data for statistical purposes is the carrying out of statistical surveys and disclosure and storage of their results.

2. Personal data collected for other than statistical purposes may be used, in the cases laid down in laws, for the preparation of official statistical information.

3. 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. 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 in laws.

#### **Article 14. Personal Data Processing for Direct Marketing Purposes**

1. Personal data may be processed for direct marketing purposes only after the data subject has given his consent.

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

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 direct marketing purposes.

4. Data controller 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 data subjects who are 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 for Electronic Communication Purposes**

The processing of personal data in the field of electronic communications shall be governed by the Law on Electronic Communications and this Law.

### **CHAPTER THREE**

### **VIDEO SURVEILLANCE**

**Article 16. Conditions on 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 ways 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 safety of persons, property or the public and in other cases when other ways or measures are insufficient and (or) inadequate for the achievement of the above mentioned purposes.

**Article 18. Requirements on Video Surveillance**

1. Processing of image data must be set down in a written data controller's document specifying the purpose and the extent of video surveillance, the retention period of video data, conditions of access to processed image data , conditions and procedure of destruction of these data and other requirements concerning legitimate processing of video data.

2. The data controller shall ensure that image data are processed only by persons authorised by the data controller who must be instructed on legal acts regulating legal protection of personal data and who obligated to abide by them by signing.

**Article 19. Installation of Video Surveillance Devices**

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

1) video surveillance covers not excessive part of the premises or territory than it is necessary;

2) image data are collected only of such an extent which is necessary.

2. It shall be prohibited to install and exploit installed video surveillance devices in such a manner that the area of surveillance covers residential premises and (or) appertain private

territory or entrance to it, except for the cases specified by laws. In the common use premises video surveillance devices may be installed on the 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 Data Subject about Video Surveillance**

1. The data controller shall ensure that the following information is clearly and properly provided before the entrance to the premises or territory in which video surveillance is used:

1) that video surveillance is used there;

2) the data controller's contact information (address or telephone number) and other requisites.

2. The data controller may provide as well other additional information relevant for ensuring that personal data are processed lawfully and without infringing the data subject's rights (e.g. purpose of video surveillance).

3. If video surveillance is used in a work place 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**

#### **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 data, including personal identification number, of data subjects who have failed to fulfil, in a timely and proper manner, their financial and (or) property obligations (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 number, to other data controllers who process consolidated debtor files (hereinafter consolidated files). The data controller may process consolidated files for the purpose of disclosing such data to third parties having legitimate interests so that they could evaluate solvency of the data subject and manage his debt only if he has duly 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 to the data subject about his default and where, within thirty calendar days of the sending (submitting) date of 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 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 files, upon receiving debtors' data from the data controller referred to in paragraph 2 of this Article, must provide each data subject with the following information (unless the data subject already has such information):

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

2) the purposes of the processing 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 being disclosed, the existence of the data subject's right of access to his personal data and his 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) settlement of the debt by the data subject;

2) the date of the debt settlement.

**Article 22. Processing of Data about the Rendered Financial Services Connected to Risk Acceptance for the Purpose of Solvency Evaluation**

1. Banks and other credit institutions as well as financial undertakings engaged in credit and (or) financial activities may disclose to each other the data subjects' to whom these banks and other credit institutions as well as financial undertakings, who are engaged with credit and (or) financial activities, have rendered or intend to render financial services concerning the acceptance of the risk (as it is laid down in the Law on Financial Institutions) (hereinafter – services) and the data subjects', providing security of obligations of the above mentioned persons' to the above mentioned institutions and undertakings, personal data (name, surname, personal identification number (data of identity document if personal identification number is not given), the type and the amount of the requested and denied financial obligations, the types, the amount and the terms of performance of existing financial obligations, data about the performance of these obligations as well as data about previous financial obligations and their performance) for the purposes of evaluation of solvency on the condition that the data subjects have given their consent.

2. Banks and other credit institutions as well as financial undertakings engaged in credit and(or) financial activities may obtain personal data on the conditions and the extent of paragraph 1 of this Article only when the data subject:

1) applies to these institutions and undertakings for the services or for the security of financial obligations;

2) has received services from these institutions and undertaking or has given security for the financial obligations and it is necessary to evaluate the existence of the risk for the proper fulfilment of the undertaken obligations.

3. Banks and other credit institutions as well as financial undertakings engaged with credit and (or) financial activities shall ensure the received data subjects' data are not:

1) processed for purposes incompatible with the purposes determined before the personal data concerned are collected;

2) stored for a period longer than twelve months, if a negative decision concerning the granting the service is taken.

4. Banks and other credit institutions as well as financial undertakings engaged with credit and (or) financial activities shall ensure that data about the services rendered, performance and proper fulfilment of them are not stored for a period longer than ten years from the date of fulfilment of these obligations, unless laws or legal acts passed on their basis establish otherwise.

## **CHAPTER FIVE**

### **RIGHTS OF THE DATA SUBJECT**

#### **Article 23. Rights of the Data Subject**

1. The data subject, in accordance with the procedure laid down in this Law, shall 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 not in compliance with 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) state security or defence;
- 2) public order and prevention, investigation, detection and 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 the 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 thirty calendar days of the date of data

subject's application. Where the request of the data subject is written, the data controller's reply must also be written.

4. The data subject may appeal against acts (omissions) of the data controller to the State Data Protection Inspectorate within three months of receipt of the reply from the data controller or within three months of the date when the time period for giving a reply referred to in paragraph 3 of this Article expires. The acts (omissions) of the State Data Protection Inspectorate may be appealed against in the court in accordance with the procedure laid down in laws.

#### **Article 24. Informing the Data Subject about the Processing of Data Relating to Him**

1. The data controller must provide the data subject from whom data relating him are collected directly, with the following information, except where the data subject already has it:

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 requisites and the address of registered office (where the data controller or its representative is a legal person);

2) the purposes of the 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; particular personal data that the data subject must provide and the consequences of his failure to provide the data, the right of the data subject to have an access to his personal data and the right to request for rectification of incorrect, incomplete and inaccurate personal data) in 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 the data subject, he must inform the data subject about that before the start of personal data processing or, if he intends to disclose the data to third parties, he must inform the data subject about that no later than by the moment when the data are disclosed for the first time, except in the cases where laws or other legal acts determine the procedure for collection or disclosure of such data and data recipients. In such case, the data controller must provide the data subject with the following information, except where the data subject already has it:

1) the identity of himself (the data controller) and his representative, if any; his permanent place of residence (where the data controller or his representative is a natural person);



or requisites and address of 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 data 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 be applicable to the processing of personal data for the statistical, historical or scientific research purposes, where the disclosure of such information is impossible or too complicated (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 in laws. The data controller must duly notify the State Data Protection Inspectorate about that 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. Data Subject's Right of Access to His Personal Data**

1. The data subject presenting to the data controller or the data processor a document certifying his identity shall have the right to obtain information on the sources and the type of his personal data that has been collected, the purpose of their processing and the data recipients to whom the data are disclosed or have been disclosed for at least the last year.

2. Having received an enquiry from the data subject concerning the processing of his personal data, the data controller must reply to data subject whether personal data relating to him are processed, and disclose to the data subject the requested data no later than within thirty calendar days of the date of the data subject's enquiry. On a request of a data subject, such data must be disclosed in writing. Once a calendar year the data controller shall disclose such data to the data subject free of charge. When such data are disclosed for a fee, the amount of the fee

shall 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. Data Subject's Right to Request Rectification, Destruction or Suspension of Further Processing of His Personal Data**

1. Where the data subject, after familiarizing with his personal data, finds that his personal data are incorrect, incomplete and inaccurate and applies to the data controller, the latter must check the personal data concerned without delay and, at a written, oral or any other request of the data subject, rectify the incorrect, incomplete and inaccurate personal data and (or) suspend processing of such personal data, except storage, without delay.

2. Where the data subject, after familiarizing 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, destroy the personal data collected unlawfully and unfairly or suspend processing of such personal data, except storage, without delay.

3. When, at the data subject's request, processing of his (her) personal data are 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 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 have to be protected.

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

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

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

7. The data controller must inform data recipients of the rectification, destruction or suspension of processing of the data subject's personal data at the request of the data subject without delay, except if the disclosure of such information is impossible or too complicated (owing to a large number of data subjects, the period covered by the data, and excessively large expenses). If such is the case, the State Data Protection Inspectorate must be notified without delay.

-

### **Article 27. Data Subject's Right to Withhold His Consent to the Processing of His Personal Data**

1. In the cases referred to in subparagraphs 1(5) and 1(6) of Article 5 of this Law, and when the 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 laid down in subparagraphs 1(5) and 1(6) of Article 5 of this Law, the data subject shall have the right to object (in writing, orally or in any other form) to the processing of his personal data. Where the objection of the data subject is legally motivated, the data controller must suspend processing of his personal data, except in the cases laid down in laws, without delay and free of charge, and duly notify the data recipients.

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

4. At the data subject's request, the data controller must notify the data subject about suspension of or refusal to suspend the processing of personal data.

-

### **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 only

by automatic means, where such a decision might have legal consequences for the data subject or affect him in other way, with the exception of the following cases:

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

2) the decision is taken when concluding or performing a contract, provided that the data subject's request to conclude or perform a contract has been granted;

3) the decision is taken when concluding or performing a contract, provided that appropriate measures have been implemented for the protection of the data subject's legitimate interests, e.g. a procedure allowing the data subject to express his opinion is established.

2. Before starting an evaluation of personal aspects of the data subject by automatic means, the data controller must provide the data subject with the conditions to access evaluation criteria and principles determined 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 other than automatic means.

### **Article 29. Assistance to the Data Subject to Exercise 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. The data subject, applying to the State Data Protection Inspectorate and presenting a document certifying his identity, shall have the right to request State Data Protection Inspectorate to collect his personal data or information on the processing of his personal data from the registered data controllers and to make the collected data or information available to him. When the data subject applies to the State Data Protection Inspectorate by electronic means, his request must be signed with a secure electronic signature. The reply to such a request shall be sent by electronic mail or, at the data subject's request, by post to the address specified in the request or shall be hand-delivered. The reply sent by electronic mail must be signed with a secure electronic signature. The State Data Protection Inspectorate must reply to the data subject's request within thirty calendar days.

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 defined in the Law on State and Official Secrets, which constitute classified information.

4. The levy of the size determined by the Government shall be taken 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 inquiry for the implementation of the right of a particular data subject to have an access to his personal data, data controllers registered in the State Register of Personal Data Controllers shall reply to the State Data Protection Inspectorate within fifteen calendar days, in accordance with the procedure established by the latter (specifying the personal data requested by the data subject or giving information of processing of his personal data, or indicating that personal data of data subject are not processed).

6. Data controllers must ensure 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 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. These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (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 the general requirements on the organisational and technical data protection measures.

3. The data controller shall process personal data himself and (or) shall authorise a data processor. Where the data controller authorises a data processor to process personal data, he 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 are 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, if such personal data are not intended for public disclosure. This obligation shall continue after leaving the public 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 meant by the employer to the employee, individual proposals of commercial character for data subjects (natural persons), the contents of which contains personal data of data subjects, including, but not limiting, the data concerning the 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 on which may be only information necessary for postal services and the contents of 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) by hand and in confidence.

8. The data controllers and persons on whose order 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 representative (pursuant to Article 1(3)(3) of this Law) in accordance with the procedure established by the Government notifies the State Data Protection Inspectorate, 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 organization;
- 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 designate person or unit to be responsible for data protection.
2. The person or unit responsible for data protection shall:
  - 1) make public the processing of personal data actions 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 on data protection;
  - 3) initiate the preparation of the notifications to the State Data Protection Inspectorate of the existence of circumstances specified 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 establishment of data protection and data processing measures and supervise implementation and use of these measures;
  - 6) undertake measures to eliminate any violations in the processing of personal data without delay;
  - 7) instruct employees authorised to process personal data on the provisions of this Law and other legal acts on personal data protection;

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

9) assist the data subjects in exercising their rights;

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

3. The data controller must provide the 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 set a reasonable term to present an opinion on the intended personal data processing.

4. The data controller must provide the person or unit responsible for data protection with the conditions to perform their functions specified in this Article independently.

5. The data controller must notify the State Data Protection Inspectorate of appointment or withdrawal of the person or unit responsible for data protection within thirty calendar days.

### **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 Articles 5(2)(6) and 5(2)(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 institutional 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 Articles 10(3), 12(1), 21(2) and 24(4) of this Law.

2. The data controller must notify the State Data Protection Inspectorate, according to the procedure established by the latter, of the cases referred to in paragraph 1 of this Article.



Such data processing may be carried out only if an authorisation has been granted by 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 of the date of receipt of the notification, except in 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 for not longer than one month, notifying the data controller about that. A decision of the State Data Protection Inspectorate to refuse an authorisation to the data controller to carry out data processing actions may be appealed against in accordance with the procedure laid down in 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 to data recipients in the European Union Member States or other countries of the European Economic Area shall be transferred on the same conditions and in accordance with the same procedure as that applicable to data recipients in the Republic of Lithuania.
2. Transfer of personal data to data recipients in third countries shall be subject to an authorisation from 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 no later than within two months from the date of the receipt of the application for 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 to transfer 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 an individual's right to private life and the protection and exercise of other rights of the data subject. Such safeguards must be stipulated in the contract on the transfer of personal data to a third country or in other document concluded 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) for important public interests or for the purpose of legal proceedings;
- 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 offences;
- 7) personal data are transferred from a public data file in accordance with the procedure laid down in laws and other legal acts.

## **CHAPTER NINE**

### **MONITORING OF IMPLEMENTATION OF THIS LAW**

**Article 36. Supervisory Authority and its Legal Status**

1. The implementation of this Law, with the exception of Article 8, shall be supervised and monitored by the State Data Protection Inspectorate. The State Data Protection Inspectorate shall be a Government institution financed from the State budget. It shall be accountable to the Government. 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 the State Data Protection Inspectorate shall be supervision of data controllers activities when processing personal data, monitoring the legality of personal data processing, prevention of violations in data processing and ensuring protection of the rights of the data subject.

4. The State Data Protection Inspectorate shall have no right to monitor processing of personal data in courts.

**Article 37. Legal Grounds and Principles of the 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 agreements to which the Republic of Lithuania is a party, this Law and other laws and legal acts.

2. Activities of the State Data Protection Inspectorate shall be based on the principles of legality, impartiality, publicity and professionalism in the discharge of its functions. When discharging its functions established by this Law and making decisions related to the discharge of the functions established by this Law, the State Data Protection Inspectorate shall be independent. Its rights may be restricted only by law.

3. State and municipal institutions and agencies, members of the Seimas, other officials, political parties, public organisations, other legal and natural persons shall have no right to exert any kind of political, economic, psychological or social pressure or other illegal influence on the director of the State Data Protection Inspectorate, civil servants and employees employed under labour contracts. Interference with the activities of the State Data Protection Inspectorate shall entail liability in accordance with laws.

**Article 38. Status of the Director of the State Data Protection Inspectorate**

1. The State Data Protection Inspectorate shall be headed by the Director of the State Data Protection Inspectorate.

2. The Director of the State Data Protection Inspectorate shall be a civil servant, the head of the institution, taken into service through competition for the period of office of five years and shall be dismissed by the Prime Minister in accordance with the procedure established in the Law on Civil Service. A person may be appointed to the post of the Director of the State Data Protection Inspectorate for not more than two periods of office.

3. The Director of the State Data Protection Inspectorate shall suspend his membership in a political party for his period of office.

4. In addition to this Law, legal status of the Director of the State Data Protection Inspectorate shall be established by the Law on Civil Service.

**Article 39. Deputy Directors of the State Data Protection Inspectorate**

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

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

3. In the absence of the Director of the State Data Protection Inspectorate, he shall, 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 activities of data controllers relating 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) examine complaints and notifications of persons (hereinafter - complaints) in accordance with the procedure laid down in this Law;

4) check the legality of personal data processing and make decisions concerning violations in personal data processing;

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

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

7) consult data controllers and draw up methodological recommendations on the protection of personal data and make them public on the Internet;

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

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

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

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

12) implement provisions of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);

13) give proposals to the Seimas, the Government, other state and municipal institutions and agencies for the drafting, amending and repealing of laws or other legal acts provided that their provisions concern issues falling within the competence of the State Data Protection Inspectorate;

14) assess personal data processing rules presented by data controllers;

15) discharge other functions established by this Law and other laws.

#### **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 and other legal and natural persons all necessary information, copies and transcripts of documents, copies of data and access to 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 personal data processing is to be checked in response to a complaint, to premises of the person being checked (including to premises leased or used on other basis), or to the territory where the documents and facilities related with the personal data processing are kept. Access to the territory, buildings and premises of the legal person (including to buildings and premises leased or used on any other basis), shall be permitted only during office hours of the legal person being checked upon presenting a certificate of 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 warranting 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 issues related to data protection;

4) to invite experts (consultants) and form work groups for examination of data processing or data protection, for the drafting of documents on data protection and for making decisions on other issues falling within the competence of the State Data Protection Inspectorate;

5) to make recommendations and give instructions to data controllers on personal data processing and protection issues;

6) to draw up records of administrative offences in accordance with the procedure laid down in 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 legal proceedings concerning violations of the provisions of international and national law on personal data protection;

9) to use photographic, video and audio recording equipment in gathering evidence during the check of lawfulness of personal data processing;

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

## **CHAPTER TEN**

### **ACCEPTABILITY AND INVESTIGATION OF COMPLAINTS**

#### **Article 42. Lodging of Complaints**

1. A person shall have the right to lodge 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 transmitted to it by other institutions.

3. Complaints shall generally be lodged in writing, including electronic format. Documents lodged by electronic means must be signed with a secure 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 on its own.

4. Oral or written enquires by persons asking for explanations, information or documents and not complaining of acts (omissions) by data controllers shall not be considered complaints.

#### **Article 43. Complaint Requirements**

1. The complaint shall contain the following information:

- 1) addressee - the State Data Protection Inspectorate;
- 2) full name and address of the complainant and, at the complainant's choice, his telephone number or electronic mail address;
- 3) name of the complainer (data controller) and address of its registered office or his residence, or address of the place where data are processed;
- 4) description, time and circumstances of the act (omission) complained about;
- 5) the complainant's application to the State Data Protection Inspectorate;
- 6) date of the complaint and the complainant's signature.

2. The complaint may be covered with the evidence available or a description of them.

3. A failure to keep to the format of a complaint referred to in paragraph 1 of this Article or give requisites shall not be the 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 to refuse to investigate the complaint within five working days of the date of receipt of the complaint and notify the data subject, provided that:

1) the investigation of the circumstances referred to in a complaint falls outside the competence of the State Data Protection Inspectorate;

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

3) a complaint on the issue has been investigated or is under investigation in court;

4) a procedural decision to start a pre-trial investigation of the subject of the complaint has already been made;

5) the text of the complaint is unreadable.

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

3. Where the complaint falls outside the competence of the State Data Protection Inspectorate, the State Data Protection Inspectorate shall, within the period referred to in paragraph 1 of this Article, transmit the complaint to the institution with the required competence and notify the complainant about that. Where the competent institution is a court, the complaint shall be sent back to complainant with the relevant information.

**Article 46. Dismiss of Investigation of a Complaint**

1. The State Data Protection Inspectorate shall dismiss the investigation of the complaint, provided that the complainant's request for the dismissal of investigation of the complaint is received. The State Data Protection Inspectorate may initiate an investigation on its own.

2. The investigation of the complaint shall be dismissed provided that the circumstances referred to in Article 45(1) occur during the investigation or in other cases laid down in this Law.

**Article 47. Request for Additional Information from the Complainant**

1. The request for documents and information necessary for the investigation of the complaint from the complainant must be lawful and motivated.



2. The complainant shall deliver the documents and information requested by the State Data Protection Inspectorate within the period specified in the request. The documents and information from the complainant may be requested repeatedly only in exceptional cases and with due justification of the necessity of these documents and information.

3. Where the complainant fails to deliver documents and information requested by the State Data Protection Inspectorate and the investigation without these documents and information is impossible, the complaint shall not be investigated.

#### **Article 48. Receipt of a Complaint**

Receipt of the 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 the civil servant of the State Data Protection Inspectorate investigating the complaint, and the reference number of the complaint. The letter confirming receipt of the complaint shall be hand-delivered to the complainant or sent to him by post or electronic mail no later than within three working days.

#### **Article 49. Complaint's Investigation Periods**

A complaint must be investigated and a reply to the complainant given within two months of the date of 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 for not longer than two months. The entire period of investigation of a complaint may not be longer than four months. The complainant shall be informed of the decision of the State Data Protection Inspectorate to extend the period of investigation of the complaint. Complaints must be investigated in the shortest possible period.

#### **Article 50. Binding 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, and to give access to all data, facilities related with the processing of personal data, and documents necessary for the discharge of its function of supervision of personal data processing.

### **Article 51. Investigation of Complaint and Decisions of the State Data Protection Inspectorate**

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

- 1) to admit the complaint as justified;
- 2) to reject the complaint;
- 3) to dismiss the investigation of the complaint.

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

3. The Decisions of the State Data Protection Inspectorate may be appealed against in a court in accordance with the procedure laid down in 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 employed under labour contracts must keep state, official, professional, commercial (trade), bank and other secrets and personal data protected by laws, which they learned in the course of their official duties, in secret.

## **CHAPTER ELEVEN**

### **LIABILITY**

#### **Article 53. Liability for Violation of this Law**

Violations of this Law shall render data controllers, data processors and other persons liable under the 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.

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

Annex to the Law of the Republic of Lithuania  
on Legal Protection of Personal Data

IMPLEMENTED LEGAL ACTS OF THE EUROPEAN UNION

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, 13 Chapter, 15 volume, p. 355).”

**Article 2. Entry into Force and Implementation of the Law**

1. This Law, with the exception of part 2 of this Article, shall enter into force on 1 January 2009.

2. The Government and the State Data Protection Inspectorate shall adopt legal acts necessary for the implementation of this Law by 1 January 2009.

3. Data controllers who, upon entry of this Law into force, continue to process, for the purposes referred to in Article 10 of the Law on Legal Protection of Personal Data, special categories of personal data related to health by automatic means, must notify the State Data Protection Inspectorate in accordance with the procedure laid down in Article 31 and 33 of the Law on Legal Protection of Personal Data referred to in Article 1 of this Law no later than within two years of the date of entry of this Law into force. This notification by the data controllers shall not suspend or terminate personal data processing operations unless the State Data Protection Inspectorate decides otherwise.

4. The Director of the State Data Protection Inspectorate taken into service before the entry into force of this Law shall, with his consent, hold the office after the entry into force of this Law. The period of office of the Director of the State Data Protection Inspectorate shall start to count from the date of entry into force of this Law.

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

**PRESIDENT OF THE REPUBLIC**

**VALDAS ADAMKUS**