

REPUBLIC OF LITHUANIA
L A W
ON LEGAL PROTECTION OF PERSONAL
DATA

21 January 2003, No. IX-1296
Vilnius

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 privacy with regard to the processing of 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 responsibility of legal and natural persons with regard to the processing of personal data.
3. This Law shall apply to the processing of personal data where:

1) personal data are processed in the course of its activities by a data controller who is established and operating on the territory of Lithuania;

2) personal data are processed by a data controller which is not established on the territory of the Republic of Lithuania but to which the laws of the Republic of Lithuania apply by virtue of international public law, including diplomatic missions and consular institutions;

3) personal data are processed by a data controller established and operating in a non-member state of the European Union, which makes use of automated 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 and the territory of the European Union. In the case specified in this subparagraph, the data controller must have its representative - an established subsidiary or a representative office in the Republic of Lithuania to which the provisions of this Law in respect of the data controller shall apply.

4. This Law shall not apply if personal data are processed by a natural person in the course of a purely personal activity, unrelated to business or profession.

5. When personal data are processed for the purposes of State security or defence, this Law shall apply in so far as other laws do not provide otherwise.

6. Free movement of personal data shall in no way be restricted or prohibited when fulfilling the commitments of membership of the Republic of Lithuania in the European Union.

7. Under this Law, regulation of legal protection of personal data in the Republic of Lithuania shall be approximated with the *acquis* referred to in the appendix to this Law.

Article 2. Definitions

1. **Personal data** - 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** - a legal or natural person to whom data are disclosed. The supervisory authorities of the implementation of this Law referred to in Articles 8 and 29 as well as state and municipal institutions and agencies shall not be regarded as recipients when they obtain personal data in response to a specific request for the purposes of discharging the functions of control provided for by law.

3. **Disclosure of data** - disclosure of personal data by transmission or making it available by any other means, with the exception of making it public in the mass media.

4. **Processing of data** - any operation, which is performed upon personal data such as collection, recording, accumulation, storage, classification, grouping, combination, 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. **Processing of data by automatic means** - operations performed upon personal data carried out in whole or in part by automated means.

6. **Data processor** - a legal or a natural person, not an employee of the data controller, processing personal data on behalf of the data controller. The data processor and/or the procedure of its appointment may be designated by laws or other legal acts.

7. **Data controller** - a legal or natural person which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes of the processing of personal data are determined by laws or other legal acts, the data controller and/or the procedure for its appointment may be designated by laws or other legal acts.

8. **Prior checking** - an advance inspection of the procedures which are planned for the processing of personal data before they are started in the cases provided for in this Law.

9. **Special categories of personal data** - the data as to the racial or ethnic origin of a natural person, his political opinions, religious, philosophical or other beliefs, membership in a trade union, and data concerning his health, sex life and criminal convictions.

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

11. **Consent** - any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to the processing of personal data relating to him. His consent with regard to special categories of personal data must be expressed clearly - in a written form, its equivalent or any other form giving an unambiguous evidence of the data subject's free will.

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

13. **Third party** - a legal or natural person, with the exception of the data subject, the data controller, the data processor and the persons who have been assigned by the data controller or the data processor to process data.

14. **Internal administration** - activity which ensures an independent functioning of the data controller (structure administration, personnel management, management and use of materials and finances, and clerical work).

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

CHAPTER TWO

PROCESSING OF PERSONAL DATA

Article 3. General Principles of Data Processing

Personal data must be:

1) collected for specified and legitimate purposes determined before collecting personal data and are later processed in a way compatible with those purposes;

2) processed accurately, fairly and lawfully;

3) accurate, and, where necessary for the processing of personal data, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing must be restricted.

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

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

2. Personal data collected for other purposes may be processed for historical, statistical or scientific purposes only in cases laid down in law provided that adequate safeguards are guaranteed by laws.

3. The controller must ensure implementation of personal data processing principles set out in paragraphs 1 and 2 of this Article.

Article 4. Storage and Destruction of Personal Data

Personal data shall not be stored longer than necessary for the purposes of data processing. Personal data shall be destroyed when no more needed for the purposes of their processing, with the exception of the data which must be transferred to State archives in cases established by law.

Article 5. Criteria for Lawful Processing of Personal Data

1. Personal data may be processed only 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 the laws to process personal data;
- 4) processing is necessary in order to protect the vital interests of the data subject;
- 5) processing is necessary for the performance of a task in the exercise of official authority vested in state and municipal institutions or a third party to whom the data are disclosed;
- 6) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party to whom the data are disclosed, except where such interests are overridden by the interests of the data subject.

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

- 1) the data subject has given his consent;
- 2) such processing is necessary for the purposes of work or public service in the exercise of the rights and obligations of the data controller in the field of labour law in cases provided by law;
- 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 because he is s legally incapable;
- 4) processing is carried out in the course of the activities by a foundation, association or any other non-profit-seeking body for political, philosophical, religious or trade-union aim on condition that the processed data relate solely to the members of the body or to persons who have regular contact with it in connection with its purposes. This

category of personal data may not be disclosed to a third party without the consent of the data subject;

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

6) it is necessary, in cases provided by law, for the prevention and investigation of criminal offences;

7) the data are necessary for a court hearing.

3. The data about a person's health may also be processed for the purposes and in the manner specified by Article 10 of this Law and the laws pertaining to health care.

4. Personal data relating to a person's record of conviction, criminal acts or security measures in the course of crime prevention or investigation also in other cases provided for by law may be processed only by a state institution or an agency following the procedure prescribed by law. Other natural or legal persons may process such data in cases specified by law provided that appropriate safeguards established by laws and other legal acts for the protection of the legitimate interests of the data subject have been implemented adequately. Detailed data about previous convictions may be processed only in accordance with the procedure set out in the Law on State Registers.

Article 6. Forms of Personal Data Disclosure

In the cases provided for by this Law personal data shall be disclosed under a personal data disclosure contract between the data controller and the data recipient in cases of multiple disclosure or under a request of the data recipient in cases of a single disclosure. The contract must specify the purposes for which the data will be used, the conditions of and the procedure for its use. The request must specify the intended use of the data.

Article 7. Use of Personal Identification Number

1. The personal identification number is a unique sequence of digits assigned to a person in accordance with the procedure set forth in the Law on the Population Register.

2. The use of a personal identification number for the processing of personal data shall be conditional on the consent of the data subject.

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

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

2) for research or statistical purposes in cases specified in Articles 12 and 13 of this Law;

3) in state registers and information systems provided that they have been officially approved under law;

4) it is used by legal persons involved in activities related to granting of loans, recovery of debts, insurance or leasing, health care and social insurance as well as in the activities of other institutions of social care, educational establishments, research and studies institutions, and when processing classified data in cases provided by law.

Article 8. Reconciliation of Processing of Personal Data with Provision of Information to the Public

The processing of personal data carried out for the purposes of providing information to the public or the purposes of artistic or literary expression as well as other purposes shall be supervised by the Inspector of Journalistic Ethics. His competencies shall be determined by the Law on Provision of Information to the Public. In these cases only the provisions of Articles 1, 2, 3, 4, 6, 7, 24, 33 and 34 of this Law shall apply to the processing of personal data.

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

Providers of social services when performing their functions related to social insurance and other purposes of social care shall provide personal data to one another without the consent of the data subject.

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

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

2. Processing of personal data for purposes of medical research shall be governed by this Law and other laws.

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

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

2. The information about the candidates, the votes received, the lists of members of the electoral committees, observers, representatives, members of initiative groups after the election, the announcement of the referendum results, as well as the lists of donors of political campaigns compiled on the basis of the statements and other documents submitted to the Central Electoral Committee by the candidates or their representatives and announced on an Internet web site may be revised after the announcement of the results of the election and the referenda for the purposes of correction of language mistakes or when the information on the Internet web site differs from the information provided in the statements and other documents at the time prescribed by legal acts. An Internet web site may not make public personal identification numbers of the candidates and any other persons, their nationality or numbers of their identification documents, the exact address (street, number of the house, number of the apartment) of their place of residence.

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

1. Personal data shall be processed in the course of scientific research on condition the data subject has given his consent. Without the consent of the data subject personal data may be processed only if the State Personal Data Protection Inspectorate which must carry out a prior checking has been duly notified.

2. The personal data which have been used for scientific research must be altered immediately in the manner which makes it impossible to identify the data subject.

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

4. In the cases where the research does not require data identifying a person, the data controller shall provide to the data recipient 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 the data subject has given his consent to have his personal data made public.

Article 13. Processing of Personal Data for Statistical Purposes

1. Processing of personal data for statistical purposes shall be carrying out of statistical surveys, disclosure and keeping of their results.

2. Personal data collected for non-statistical purposes may be used, in the cases provided for by law, for the preparation of official statistical information.

3. Personal data collected for statistical purposes may be disclosed and used for non-statistical purposes in accordance with the procedure and cases set out in the Law on Statistics.

4. Personal data collected for different statistical purposes shall be compared and combined only where protection of personal data against the unlawful use for non-statistical purposes is ensured.

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 provided by law.

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

1. Personal data may be processed for the purposes of direct marketing only if the time period for the storage of personal data is set during the collection of the data.

2. Personal data may be processed for the purposes of direct marketing provided that the data subject has given his consent.

Article 15. Processing of Personal Data in Telecommunications

The processing of personal data in telecommunications shall be governed by the Law on Telecommunications and this Law.

Article 16. Processing of Personal Data for the Purposes of Evaluation of a Person's Solvency and Management of His Debt

1. The data controllers shall have the right to process and disclose to third parties having the legitimate interests the data as well as the personal identification number of the data subjects who have failed to fulfil in a timely and proper manner their financial and/or property obligations (hereinafter "debtors") for the purposes of evaluation of the person's

solvency and debt management, provided that all the 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 the debtors' personal data and personal identification number to data controllers processing consolidated debtor files (hereinafter "consolidated files"). The data controller may process consolidated files with a view to disclosing such data to third parties having the legitimate interests so that they could evaluate solvency of the data subject and manage the debt only if he has duly notified, following the procedure set out in Article 26 of this Law, the State Data Protection Inspectorate which must carry out a prior checking.

3. The data controller may disclose the debtors' personal data on condition he has sent a reminder in writing to the data subject about his default on the debt and where, within 18 calendar days of the date when the data controller sent/submitted to the data subject a reminder:

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

2) the data subject did 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 the files of other personal data which were compiled and are processed for purposes other than evaluation of solvency and debt management.

6. The data controller who is processing consolidated files, upon receiving from the data controller referred to in paragraph 2 of this Article the debtors' data, must provide to each data subject the following information, except where the data subject already has such information:

1) the identity of himself (the data controller) and his representative if any, and his registered office;

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

3) the sources and type of the data subject's personal data which have been collected, the recipient and the purposes for which the data are being disclosed, 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 the data subject on a timely and proper fulfilment of his financial and/or property obligations may not be processed for a period longer than 10 years from the date of the settlement of the debt. Where the data subject repays his

debt, data controllers must ensure that during the processing of the data about the data subject's default on a 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 data of the debt settlement.

8. Banks and other credit institutions and financial undertakings engaged in credit and/or financial activities may disclose to each other the following data of the data subjects who have taken out loans from them, including leasing/financial leasing: the name, surname, personal identification number, the type of the loan, its amount and the deadline for the repayment of the loan in order to evaluate the solvency of the subjects. Banks and other credit institutions and financial undertakings engaged in credit and/or financial activities may apply to each other with a request to obtain the personal data referred to in this paragraph only when the data subject applies to these institutions for a loan, including leasing/financial leasing, and gives his consent that these institutions and undertakings obtain his data. The data of the data subjects may not be:

- 1) stored for a period longer than 2 working days of the receipt of such data;
- 2) combined with the other personal data.

CHAPTER THREE

RIGHTS OF THE DATA SUBJECT

Article 17. Rights of the Data Subject

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

- 1) to know/ be informed about the processing of his personal data;
- 2) to have access to his personal data and familiarise himself with the processing method;
- 3) to demand rectification or destruction of his personal data or restriction 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 to the processing of his personal data.

2. The data controller must provide conditions for the data subject to exercise the rights specified in this Article, with the exception of cases provided by law when it is necessary to ensure:

- 1) state security or defence;
- 2) public order, the prevention, investigation, detection and prosecution of criminal offences;
- 3) important economic or financial interests of the state;
- 4) prevention, investigation and detection of breaches of official or professional ethics;
- 5) protection of the rights and freedoms of the data subject or any other persons.

3. The data controller must give a reasoned refusal to grant the request of the data subject to exercise the rights granted by this Law to the data subject. Upon receiving a request from the data subject, the data controller must send a reply to him within 30 calendar days of the date of the data subject's application. Where the request of the data subject is in writing, the data controller must send him a written reply.

4. The data subject may appeal the acts/omissions of the data controller to the State Data Protection Inspectorate within 3 months of the receipt of the reply from the data controller or within 3 months of the date when the time period for giving a reply set out in paragraph 3 of this Article expires. The acts/omissions of the State Data Protection Inspectorate may be appealed against in court in accordance with the procedure provided by law.

Article 18. Informing the Data Subject about the Processing of Data Relating to Him

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

- 1) the identity of the data controller and his representative if any, and his permanent place of residence where the data controller or his representative is a natural person, or other particulars, and the 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) any other additional information - the recipient of the data and for what purposes the data of the data subject are disclosed; what personal data the data subject is supposed to provide and the consequences of his failure to provide data, the right of the data subject to have access to his personal data and the right to request rectification of

incorrect, incomplete and inaccurate personal data, necessary for ensuring a proper processing of personal data without violation of 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 it before the start of data processing or, if he intends to disclose the data to third parties, he must inform the data subject about it not later than by the moment when the data are disclosed for the first time, unless the laws or other legal acts determine the procedure for collection or disclosure of such data and the data recipients. In such cases the data controller must provide to the data subject the following information except where the data subject already has such information:

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 other particulars and 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 personal data of the data subject;

3) any other additional information (the sources and type of his personal data which is being collected or will be collected; the recipient of the data subject's personal data and the purposes of the disclosure; the right of the data subject to have access to his personal data and his right to request rectification of incorrect, incomplete and inaccurate personal data) to the extent it is necessary to ensure a fair processing of personal data without violating the rights of the data subject.

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 the data of the data subject he must inform the data subject about the recipient of the personal data and the purposes for which the data will be disclosed.

4. Paragraph 2 of this Article shall not be applicable to the processing of personal data for the statistical or research purposes where the provision of such information is impossible or involves unnecessary difficulties 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 data are established by law. The data controller must duly notify the State Data Protection Inspectorate about it following the procedure set out in Article 26 of this Law.

Article 19. Data Subject's Right of Access to his Personal Data

1. Upon submitting to the data controller or the data processor a document certifying his identity, the data subject shall be entitled to obtain information on the source and type of his personal data that has been collected, the purposes of processing, and the recipient to whom the data are disclosed.

2. Upon receiving an enquiry from the data subject concerning the processing of his data, the data controller must make a reply whether the personal data relating to him are processed, and provide to the data subject the requested data within 30 calendar days of the date of the receipt of the data subject's enquiry. On request such information must be provided to the data subject in writing. Once a calendar year the data controller shall provide such information to the data subject free of charge. When such information is disclosed for a fee, the amount of the fee shall not exceed the expenses of the disclosure of the data. The procedure of compensation of the expenses of disclosure of the data shall be determined by the Government.

Article 20. The Data Subject's Right to Request Rectification, Destruction of His Personal Data or Restriction of Further Processing of His Personal Data

1. Where the data subject, after access to his personal data, finds that his data are incorrect, incomplete and inaccurate and applies to the data controller, the latter must check the personal data without delay and, at the request of the data subject, oral or written or in any other form, immediately rectify the incorrect, incomplete and inaccurate personal data and/or restrict further processing of such personal data except its keeping.

2. Where the data subject, after access to his personal data, considers that his 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 the data subject's request in writing, immediately destroy the personal data collected unlawfully and unfairly or restrict further processing of such personal data except its keeping.

3. When, upon the request of the data subject, further processing of his personal data is restricted, the personal data further processing of which has been restricted must be kept until their rectification or destruction either at the request of the data subject or upon expiry of the period of their keeping. Any other actions of processing of such personal data may be performed solely:

1) for the purposes of giving proof of the circumstances due to which further processing of the data was restricted;

2) where the data subject gives his consent for the 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 immediately notify the data subject of the performed or not performed rectification, destruction of the personal data or restriction of their further processing in response to the application of the data subject.

5. Personal data shall be rectified and destroyed or their further processing shall be restricted in response to the application of the data subject and on the basis of documents confirming his identity and his personal data.

6. If the data controller questions the correctness of the personal data submitted by the data subject, he must restrict further processing of such personal data, check the data and update them. The contested personal data may be used solely for checking their correctness.

7. The data controller must inform forthwith data recipients of the personal data rectified or destroyed and of the restriction of further processing at the request of the data subject except where providing such information might be impossible or too difficult due to an excessively large number of the data subjects, the period covered by the data and unreasonably high costs. If such is the case, the State Data Protection Inspectorate must be immediately notified.

Article 21. Data Subject's Right to Withhold His Consent to the Processing of His Personal Data

1. In the cases referred to in paragraph 1(5) and (6) of Article 5 of this Law, and when the data are being processed or are about 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 paragraph 1(5) and (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 immediately and free of charge restrict any other further processing of personal data except in the cases set out by law, 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 processed or are about to be processed for the purposes of direct marketing. In this case the data controller must immediately and free of charge restrict any further processing of personal data except in the cases provided for by law and must duly notify the recipients of the data.

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

Article 22. Evaluation of Personal Aspects by Automated Means

1. No decision may be taken in respect of the data subject's personal aspects (his creditworthiness, reliability, performance at work) where such aspects were evaluated only by automated means and where such a decision might produce legal effects concerning the data subject or affect him in any other way, with the exception of the following cases:

1) the decision is taken following the procedure established by law, where laws provide for measures for the protection of the legitimate interests of the data subject;

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

3) the decision is taken when concluding a contract or performing it provided that appropriate measures have been implemented for the protection of the legitimate interests of the data subject, e.g., a procedure has been provided allowing the data subject to put his point of view.

2. Before undertaking the evaluation of the personal aspects of the data subject by automated means, the data controller must provide conditions for the data subject to be informed about the evaluation criteria and principles determined by the data controller.

3. Where, following the evaluation of the personal aspects of the data subject by the data controller by automated means, the data subject objects to such an evaluation he shall be entitled to put his point of view about the evaluation of his personal aspects. The data controller must take into account the point of view of the data subject and, as necessary, repeat the evaluation by non-automated means.

Article 23. Service 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. When applying to the State Data Protection Inspectorate and after producing his identity document, the data subject shall have the right to request the State Data Protection Inspectorate to collect his personal data or information on the processing of his personal data from registered data controllers and to make the collected data or information available to him.

3. When providing to the data subject the service referred to in paragraph 2 of this Article, the State Data Protection Inspectorate shall not have the right to collect data which is classified information under the Law of the Republic of Lithuania on State and Official Secrets.

4. The fee determined by the Government shall be taken for the service to the data subject specified in paragraph 2 of this Article.

CHAPTER FOUR SECURITY OF DATA

Article 24. 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 any accidental or unlawful destruction, alteration, disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the data to be protected and the risks represented by the processing and must be specified in a written document or its equivalent (data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor etc.).

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

3. When authorising the data processor to process personal data, the data controller shall stipulate that personal data must be processed only on instructions from the data controller.

4. The relations between the data controller and the data processor who is not the data controller shall be regulated by a written contract except where such relations are provided for by laws or other legal acts.

5. The employees of the data controller, the data processor and their representatives who are processing personal data must keep confidentiality of personal data if these personal data are not intended for public disclosure. This obligation shall continue after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

CHAPTER FIVE

REGISTRATION OF DATA CONTROLLERS

Article 25. Notification of Data Processing

1. Personal data may be processed by automated means subject to notification by the data controller or his representative of the State Data Protection Inspectorate (pursuant to paragraph 3(3), Article 1 of this Law) in accordance with the procedure established by the Government, except when personal data are processed:

- 1) for the purposes of internal administration;
- 2) processing is carried out in the course of the activities by a foundation, association or any other non-profit-seeking body for political, philosophical or trade union aim on condition that the processed data relate solely to the members of the body or to persons who have regular contact with it in connection with its purposes;
- 3) in the cases specified in Article 8 of this Law;
- 4) in the cases specified in Article 10 of this Law;
- 5) following the procedure set forth in the Law of the Republic of Lithuania on State and Official Secrets.

Article 26. 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 automated means save for the purposes of internal administration or in the cases specified in Article 10 and paragraph 2(6) and (7) of Article 5 of this Law;

2) where the data controller intends to process by automated means public data files unless the laws and other legal acts specify the procedure for disclosure of the data;

3) where the data controller of the information systems of state registers or state and municipal institutions authorises the data processor to process personal data save the cases where the laws and other legal acts provide for the right of the data controller to authorise a specific data processor to process personal data or where the data processor is a legal entity established by the data controller;

4) in the cases specified in paragraph 1 of Article 12, paragraph 2 of Article 16 and paragraph 4 of Article 18 of this Law.

2. The data controller must, two months before the intended commencement of the data processing operations, notify the State Data Protection Inspectorate, in accordance with the procedure specified by the State Data Protection Inspectorate, about the cases referred to in paragraph 1 of this Article. Such data processing operations may be carried out only if an authorisation has been granted by the State Data Protection Inspectorate. Within two months of the receipt of the notification, the State Data Protection Inspectorate must carry out prior checking according to the procedure determined by the State Data Protection Inspectorate and grant or refuse to grant an authorisation to the data controller to carry out data processing operations. A decision of the State Data Protection Inspectorate not to grant an authorisation to the data controller to undertake data processing operations may be appealed against following the procedure prescribed by law. If, within two months of the date of the receipt of the notification specified in this paragraph, the State Data Protection Inspectorate fails to take a decision in respect of granting or refusal to grant an authorisation it shall be regarded that the data controller has been granted an authorisation to carry out data processing operations about which a notification had been made.

Article 27. 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 SIX

TRANSFER OF PERSONAL DATA TO DATA RECIPIENTS

IN THIRD COUNTRIES

Article 28. Transfer of Personal Data to Data Recipients in Third Countries

1. Transfer of personal data to recipients in foreign countries shall be subject to an authorisation from the State Data Protection Inspectorate, except in the cases referred to in paragraph 4 of this Article.

2. The State Data Protection Inspectorate shall grant an authorisation for transfer of personal data to foreign countries, provided that there is an adequate level of personal data protection in these countries. The level of legal protection of personal data shall be assessed in the light of all circumstances surrounding a data transfer operation, by giving particular consideration to the laws and other legal acts in force in the country of destination providing legal protection of personal data, the nature of the data, the proposed processing operations, purposes of processing, its duration and safeguards which shall be observed in the third country in question.

3. 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 safeguards for the protection of an individual's right to privacy as well for protection and exercise of the other rights of the data subject. Such safeguards must be stipulated in the contract on the transfer of personal data to a third country.

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

- 1) the data subject has given his consent to the transfer of the 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 concluded 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 the implementation of pre-contractual measures taken in response to the data subject's request;
- 4) the transfer of personal data is necessary or legally required in the public interest or for the purpose of legal proceedings;
- 5) the transfer is necessary in order to protect the vital interests of the data subject;
- 6) the transfer is necessary for the prevention or investigation of criminal offences;

7) the data are transferred from a public data file following the procedure prescribed by laws and other legal acts.

CHAPTER SEVEN

MONITORING OF APPLICATION OF THIS LAW

Article 29. Supervisory Authority

1. The implementation of the Law on Legal Protection of Personal Data, 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 major objectives of the State Data Protection Inspectorate shall be supervision of the activities of data controllers when processing personal data, monitoring the legality of processing of personal data, prevention of breaches in data processing and ensuring protection of the rights of the data subject.

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

Article 30. Legal Basis ands Principals 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 legal acts.

2. The activities of the State Data Protection Inspectorate shall be based on the principles of lawfulness, impartiality, openness and professionalism in the discharge of its functions. When discharging the functions provided by this Law and making its decisions related to the discharge of the functions set out for it in this Law, the State Data Protection Inspectorate shall be independent; its rights may be limited only by law.

3. State and municipal institutions and agencies, members of the Seimas and other officials, political parties, political and public organisations, other legal and natural persons shall have no right to exert any kind of political, economic, psychological or social pressure on the employees of the State Data Protection Inspectorat or tamper with them in any other way. Interference with the activities of the State Data Protection Inspectorate shall render the infringing party liable in accordance with law.

Article 31. Functions of the State Data Protection Inspectorate

The State Data Protection Inspectorate shall:

- 1) administer the Register of Personal Data Controllers, make its data public and carry out supervision of the activities of the registered data controllers relating to the processing of personal data;
- 2) examine personal requests and complaints in cases provided by this Law in the manner set forth in the Law on Public Administration;
- 3) check the lawfulness of personal data processing and take decisions in respect of the breaches of personal data processing;
- 4) grant authorisations to data controllers to disclose personal data to data recipients in third countries;
- 5) draw up and announce annual reports on its activities;
- 6) provide assistance to data controllers and draw up methodological recommendations on the protection of personal data and make them public on the internet;
- 7) following the procedure established by law, provide assistance to data subjects residing abroad;
- 8) provide information, in the cases established by law, to other states about the legislation of the Republic of Lithuania regulating protection of personal data and the practices of its administration;
- 9) carry out prior checking in the cases established by this Law and submit its conclusions to the data controller about the intended data processing;
- 10) implement the provisions of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);
- 11) make recommendations to the Seimas, the Government, other state and municipal institutions and agencies relating to drafting, amendment and repeal of laws or other legal acts where the provisions of laws or other legal acts are related to the questions falling within the competence of the State Data Protection Inspectorate;
- 12) assess the personal data processing regulations submitted by data controllers;
- 13) perform other functions set out in this Law and other legal acts.

Article 32. Rights of the State Data Protection Inspectorate

1. The State Data Protection Inspectorate shall be empowered:

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 and get access to all data and documents necessary for discharging all the functions of supervision of personal data processing;

2) to obtain access, subject to a prior notice in writing, to the premises of the supervised person, including the premises which are leased or used on any other basis, or to the territory where the documents and equipment used for the personal data processing are kept. Access to the territory of the legal person, his buildings and premises, including the buildings and premises which are leased or used on any other basis shall be permitted only during the office hours of the legal person under supervision. Access to residential premises, including the premises which are leased or used on any other basis of a natural person under supervision, where documents and equipment relating to the personal data processing are kept shall be permitted only upon producing a court order warranting entry into the residential premises;

3) to take part in the sessions of the Seimas, meetings of the Government and other state institutions when issues relating to the personal data protection are being deliberated;

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

5) to make recommendations and give instructions to data controllers with regard to personal data processing and protection;

6) to draw up records about administrative offences in accordance with the procedure set out in the Code of Administrative Offences

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

8) to take part in legal proceedings involving violations of international and national law on personal data protection;

9) to exercise other rights provided by law and other legal acts.

CHAPTER EIGHT

LIABILITY

Article 33. Liability for Breaches of this Law

Breaches of this Law shall render data controllers, data processors and other persons liable under the laws the Republic of Lithuania.

Article 34. 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 or omissions by the data controller, the data processor or any other persons in violation of 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 court.

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

The Law of the Republic of Lithuania on Legal Protection of Personal Data has been approximated with 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.”

Article 2. Entry into Force

1. This Law, with the exception of paragraph 3(3) and paragraph 6 of Article 1, and Article 23 shall enter into force on 1 July 2003.

2. Paragraph 3(3) and paragraph 6 of Article 1 of this Law shall enter into force upon Lithuania’s accession to the European Union.

3. Article 23 of this Law shall enter into force on 1 April 2004.

4. Upon Lithuania’s accession to the European Union, Article 28 of this Law shall apply only to the transfer of personal data to the countries which are non-member states of the European Union.

Article 3. Implementation of the Law

1. Within three months from entry of this Law into force, the Government shall submit to the Seimas draft laws amending the laws relating to the implementation of this Law.

2. By 1 July 2003 the Government shall approve the legal acts necessary for the implementation of this Law.

3. The data controllers who, upon entry of this Law into force, continue the data processing operations in the cases specified in Article 26(1) must notify about it the State Data Protection Inspectorate within 6 months of the date of entry of this Law into force. The notification made by the data controllers shall not suspend or revoke the data processing operations unless the State Data Protection Inspectorate decides otherwise.

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

PRESIDENT OF THE REPUBLIC

VALDAS ADAMKUS