

LAW ON LEGAL PROTECTION OF PERSONAL DATA

• CHAPTER I. GENERAL PROVISIONS	2
• Article 1. Purpose, Objectives and Scope of the Law	2
• Article 2. Definitions	3
• CHAPTER II. PROCESSING OF PERSONAL DATA	4
• Article 3. Duties of the Data Controller	4
• Article 4. Storage and Destruction of Personal Data	4
• Article 5. Criteria for Lawful Processing of Personal Data	4
• Article 6. Forms of Personal Data Disclosure	5
• Article 7. The Use of Personal Identification Number	5
• Article 8. Reconciliation of Processing of Personal Data and Providing Information to the Public	6
• Article 9. Processing of Personal Data for Purposes of Social Care	6
• Article 10. Processing of Personal Data for Purposes of Health	6
• Article 10.1 Processing of Personal Data for Elections, for Referendum, for Purposes of the Citizen Legislation Initiative	6
• Article 11. Processing of Personal Data for the Purposes of Scientific Research	7
• Article 12. Processing of Personal Data for Statistical Purposes	7
• Article 13. Processing of Personal Data for the Purposes of Direct Marketing	8
• Article 14. Processing of Personal Data in the Field of Telecommunications	8
• CHAPTER III. RIGHTS OF THE DATA SUBJECT	9
• Article 15. Rights of the Data Subject	9
• Article 16. Informing the Data Subject about the Processing of Data Relating to Him	9
• Article 17. Data Subject's Right of Access to his Personal Data	10
• Article 18. The Data Subject's Right to Request Rectification or Destruction of his Personal Data	10
• Article 19. Data Subject's Right to Object to the Processing of His Personal	11
• Article 20. Service to the Data Subject	11
• CHAPTER IV. SECURITY OF DATA	12
• Article 21. Security of Data	12
• CHAPTER V. REGISTRATION OF DATA CONTROLLERS	12
• Article 22. Notification of Data Processing	12
• Article 23. Registration of Data Controllers	13
• CHAPTER VI. TRANSFER OF PERSONAL DATA TO DATA RECIPIENTS IN FOREIGN COUNTRIES	13

• Article 24. Transfer of Personal Data to Data Recipients in Foreign Countries	13
• CHAPTER VII. MONITORING OF APPLICATION OF THIS LAW	14
• Article 25. Supervisory Authority	14
• Article 26. Functions of the Supervisory Authority	14
• Article 27. Rights of the Supervisory Authority	15
• CHAPTER VIII. LIABILITY	15
• Article 28. Liability for Breaches of this Law	15
• Article 29. Compensation for Material and Non-Material Damage	16
.....	16

11 June 1996, No. I-1374

New version 17 July 2000, No. VIII-1852

As last amended on 20 June 2002, No. IX-970

Vilnius

CHAPTER I. GENERAL PROVISIONS ➔

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

1. The purpose of this Law shall be protection of the right of inviolability of the person's private life related to the processing of personal data and creation of the conditions for a free movement of personal data.

2. This Law shall regulate relations arising due to 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, and codes. The Law shall establish the rights of natural persons as data subjects, the procedure of protection of these rights, the rights, duties and responsibility of legal and natural persons with regard to processing of personal data.

3. This Law shall apply to:

1) legal and natural persons which process personal data in the territory of the Republic of Lithuania;

2) a representative of the data controller in the Republic of Lithuania if the data controller operating in a non-member state of the European Union makes use of automatic personal data processing equipment established in the Republic of Lithuania unless such equipment is used only for purposes of transit through the territory of the European Union; in this case the same provisions of this Law shall apply to the representative as to the data controller.

4. This Law shall not apply where personal data are processed by a natural person solely in the course of private activities.

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.

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 an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
2. Special categories of personal data shall mean 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 or a political party, and data concerning his health, sex life and criminal convictions.
3. Data controller shall mean a legal or natural person which alone or jointly with others determines the purposes and means of the processing of personal data, and processes personal data.
4. Data processor shall mean a legal or natural person which processes personal data on behalf of the data controller.
5. Data recipient shall mean a legal or natural person to whom data are disclosed. The supervisory authority of the implementation of this Law referred to in Articles 8 and 25 as well as the Communications Regulatory Authority referred to in Article 14 shall not be regarded as recipients when they obtain personal data for purposes of checking of the processing.
6. Consent shall mean 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 shall be made in writing, and his consent with regard to any other data - in any other form.
7. Third party shall mean a legal or natural person, with the exception of the data subject, the data controller, and the data processor.
8. Processing of data shall mean any operation which is performed upon personal data such as collection, recording, accumulation, storage, classification, organisation, combination, adaptation (supplementing or alteration), making available, disclosure, use, holding, logical and/or arithmetic operations, retrieval, dissemination, destruction or any other operation or a set of operations.
9. Disclosure of data shall mean making data available, its transmission or creating conditions to access personal data by various means.
10. Filing system shall mean 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. Internal administration shall mean activity which ensures an independent functioning of the data controller (structure administration, personnel management, management and use of materials and finances, and management of clerical work).
12. Prior checking shall mean an advance inspection of the procedures which are planned for the processing of personal data with the aim of determining their effectiveness and reliability.

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

CHAPTER II. PROCESSING OF PERSONAL DATA ➔

Article 3. Duties of the Data Controller ➔

It shall be for the data controller to ensure that personal data are:

- 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;
- 4) not excessive in relation to the purposes of personal data processing;
- 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.

Article 4. Storage and Destruction of Personal Data ➔

1. 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.

. 2. The procedure of transfer of personal data to State archives shall be determined by the Lithuanian Archives Department.

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) processing is necessary for entering into contract or the performance of a contract to which the data subject is party;
- 3) processing is necessary for compliance with a legal obligation to which the data controller is subject;
- 4) processing is necessary in order to protect the life of the data subject and where the data subject is incapable of giving his consent;
- 5) processing is necessary in the exercise of official authority vested by the institutions of state governance and administration and local government institutions in the data controller or in 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. Special categories of personal data may be processed only if:

1) the data subject has given his consent in writing;

2) processing is necessary for the purposes of work or in the exercise of public service in carrying out the rights and obligations of the data controller in the field of employment law in the cases provided by law or other legal acts;

3) it is necessary to protect the life of the data subject or of another person, where the data subject is unable to give his consent or is legally incapable;

4) processing is carried out in the course of its activities by a foundation, association, trade union, political party or any other non-profit-seeking body on condition that the processing relates solely to the members of the body or to persons who take part in its activities in some other way and that the data are not disclosed to a third party without the consent of the data subjects;

5) the data are 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 (its condition, diagnosis, prognosis and treatment) may also be processed for the purposes and in the manner specified by Article 10 of this Law and the laws pertaining to the field of health care.

4. Personal data collected for other purposes may be processed for historical or research purposes on condition adequate safeguards have been established.

Article 6. Forms of Personal Data Disclosure ➡

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

Article 7. The 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. Only the provisions of this Article shall apply to the use of the Register.

2. The personal identification number may be used without the consent of the data subject when:

- 1) such a right is stipulated in laws or other legal acts;
- 2) carrying out research or for statistical purposes. In this case the provisions of Articles 11 and 12 shall be applied respectively;
- 3) it is used at institutions, agencies and enterprises 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 institutions, institutions of science and learning, and when processing classified data in cases provided by law.

Article 8. Reconciliation of Processing of Personal Data and Providing Information to the Public ➡

The processing of personal data carried out solely for journalistic purposes or the purposes of artistic or literary expression as well as other purposes of providing information to the public shall be supervised by the institutions specified in the Law on Provision of Information to the Public. In these cases only the provisions of Articles 1, 2, 3, 4, 7, 21, 28 and 29 of this Law shall apply to the processing of personal data.

Article 9. Processing of Personal Data for Purposes of 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 ➡

1. Personal data on the person's health (its state, diagnosis, prognosis and treatment) may be processed by a health care professional. Under the laws regulating the health care system or patients' rights, the Government resolutions and legal acts of the Ministry of Health, this professional must keep the secret of the person's health.

2. Data on the person's health (its state, diagnosis, prognosis and treatment) may be processed for the following purposes:

- 1) preventive (prophylactic) medicine;
- 2) medical diagnostics;
- 3) provision of health care and treatment;
- 4) management of the health-care system.

3. Personal data for the purposes of medical research shall be processed in conformity with the Law on Ethics of Biomedical Research.

Article 10.1 Processing of Personal Data for Elections, for Referendum, for Purposes of the Citizen Legislation Initiative ➡

1. The processing of personal data (name, surname, date of birth, personal number, address of living place, citizenship, the number of personal identification document) for the

purposes of elections, referendums, citizen legislation initiative, politic campaigns, sponsorship of politic parties is determined by this and other laws.

2. Information, compiled by the Chief Election Commission according to the requisitions and other documents presented by the candidates or their representatives and announced in the Internet site, about the candidates, also about the votes they get, the lists of election, referendum committees' members, observers, representatives, the members of initiative groups after the announcement of elections, referendum results, the lists of political campaign benefactors after their announcement can be changed only making corrections of language or when the information in the Internet site differs from the information presented in requisitions or other documents at the time defined by the acts of legislation. The personal numbers of candidates and other persons, the numbers of citizenship or personal identification documents, exact address of living place (street, house and appartament number) can't be announced in the Internet site.

Article 11. Processing of Personal Data for the Purposes of Scientific Research ➡

1. While carrying out scientific research, personal data shall be processed without the consent of the data subject only where the research cannot be carried out without identifying a person. In such cases the program of research must be approved by the Government or a body authorised by it.

2. The personal data which have been used for scientific research must be altered forthwith 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 provided the data subject has given his consent.

Article 12. 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 for the preparation of official statistical information unless this Law and other laws provide otherwise.

3. Personal data collected for statistical purposes may be disclosed and used for non-statistical purposes in accordance with the procedure and cases established 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 established by law.

Article 13. Processing of Personal Data for the Purposes of Direct Marketing ➡

1. Personal data may be processed for the purposes of direct marketing, provided the time period of the storage of personal data is set during the collection of the data.
2. Personal data shall not be processed for the purposes of direct marketing if the data subject has not given his consent to the processing of his personal data. The data subject shall be informed about his right to object to the processing of his personal data.

Article 14. Processing of Personal Data in the Field of Telecommunications ➡

1. The processing of personal data in the field of telecommunications shall be the processing of personal data related to the provision of public telecommunications services on public telecommunications networks, in particular on the Integrated Services Digital Network and Public Mobile Digital Networks.

2. Personal data shall not be processed in public lists of subscribers, if the data subject objects to the processing of his personal data. The data controller or data processor must inform the data subject about his right to object to the processing of his personal data.

3. Subject to the consent of the subscriber (the data subject), the public lists of subscribers, printed or electronic, shall only specify the name and surname, telephone number and address of the subscriber. Where the subscriber does not give his consent, data controllers (the provider of telecommunications services and the operator of telecommunications) must not disclose his personal data. In public electronic lists of subscribers, the search of personal data according to a subscriber's telephone number shall not be permitted. It shall be prohibited to provide the personal data of the subscriber according to his telephone number to third parties unless the laws of the Republic of Lithuania provide otherwise.

4. The subscriber shall be issued an itemised bill for telecommunications services on request. The provider of telecommunications services or the operator of telecommunications networks must specify in the bill the number called, the type of conversation or service, the starting time (date and time), duration and charge for the calls made or services used.

5. Data flow relating to the subscriber of public telecommunications services (subscriber's number, subscriber's address and number called, the type of conversation or service, the starting time and duration of the calls made or services provided) shall be kept as long as it necessary for the purposes for which it has been collected and processed, and if other laws do not provide otherwise it must be destroyed not later than after the lapse of three years after the termination of the call or made such so as to make direct or indirect identification of the person impossible.

6. Employees of companies providing telecommunications services shall have the right to process data flow and billing specified in paragraphs 4 and 5 of this Article only to the extent necessary to carry out their duties.

7. The Communications Regulatory Authority shall be entitled to receive data flow specified

in paragraph 4 of this Article for resolving disputes between providers of public telecommunications services and their subscribers.

8. Data controllers (provider of telecommunications services and operator of telecommunications) must ensure security of the telecommunications network in accordance with the procedure provided in Article 21 of this Law. In the event of threat of damage to the telecommunications network or its part, the provider of public telecommunications services shall inform its subscribers using the services provided on the network or its part about the possible threat to the security of the network.

CHAPTER III. RIGHTS OF THE DATA SUBJECT ➡

Article 15. Rights of the Data Subject ➡

1. The data subject, in accordance with the procedure provided by laws, shall be entitled:

- 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 in the cases established in paragraph 1 of Article 18;
- 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) detection of breaches of official or professional ethics;
- 5) 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 submitted to him in writing by the data subject and must send an appropriate written notice to him. The data subject may appeal the refusal of the data controller within 30 calendar days after its receipt to the institution authorised by the Government, and the refusal of the institution authorised by Government may be appealed against in the court in the manner set out by law.

Article 16. 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 to himself are collected directly with the information on the identity of himself (the data controller) and his representative if any, and his permanent place of residence or registered office, the

purposes of the processing and the recipient of the data, except where the data subject already has such information.

2. Where the data controller collects personal data not from the data subject he must inform the data subject about it before the start of data processing unless the laws or other legal acts lay down the procedure for collection or disclosure of such data. In such cases the data controller must provide the data subject with information on the identity of himself (the data controller) and his representative if any, his permanent place of residence or registered office, also the sources and type of his personal data which are being or will be collected, the purposes of the processing or the intended processing, and the recipient or the intended recipient of the data, except where the data subject already has such information.

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, he must inform the data subject before disclosing data of the data subject to third parties for the first time.

Article 17. Data Subject's Right of Access to his Personal Data ➡

1. Upon submitting a document certifying his identity, the data subject shall be entitled to obtain information on the source and type of his personal data, 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 reply whether the personal data relating to him are processed, and provide to the data subject the requested data within 30 calendar days from the day of the receipt of the data subject's request. On request such information shall 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 provided for a fee, the fee shall not exceed the expenses of the disclosure of the data. The Government or a body authorised by it shall determine the procedure of payment.

Article 18. The Data Subject's Right to Request Rectification or Destruction of his Personal Data ➡

1. If the data subject considers that his data are incorrect, incomplete and inaccurate and applies to the data controller, the latter must check and rectify the personal data. If the data subject considers that his data are processed unlawfully and unfairly and applies to the data controller, the latter must check free of charge the lawfulness of the processing of personal data and, at the request of the data subject, destroy the data collected unlawfully and unfairly.

2. The data controller must immediately notify the data subject of the performed or not performed rectification or destruction of the personal data in response to the application (request) of the data subject.

3. Personal data shall be rectified and destroyed in response to the application (request) of the data subject and on the basis of documents confirming his identity and his personal data .

4. 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

rectify it. The contested personal data may be used solely for checking their correctness.

5. The data controller must inform data recipients of the personal data rectified or destroyed at the request of the data subject.

6. The data controller must keep for at least 3 years all the records of personal data rectified at the request of the data subject in such a manner that they could be retrieved when necessary.

Article 19. Data Subject's Right to Object to the Processing of His Personal ➡

Data 1. In the cases referred to in subparagraphs 1, 2, 5 and 6, paragraph 1 and subparagraphs 1 and 4, paragraph 2, Article 5 of this Law, and when the data are being processed or it is envisaged to process them for the purposes of direct marketing, the data controller shall inform the data subject about his right to object (also to withhold his consent) to the processing of his personal data at no cost.

2. The data subject shall be entitled to give or not to give his consent, or to withhold his consent to the processing of personal data relating to him when the processing of data is carried out on the data controller's initiative. The objection and the request to withhold the given consent shall be laid down in writing.

3. When the data controller evaluates by automatic means certain personal aspects relating to the data subject and the data subject objects to such an evaluation, the data controller must provide facilities for the data subject to familiarise himself with the method of evaluation established by the data controller. The data subject shall have the right to express his opinion on the evaluation of the data and the method used for that, and the data controller must take the opinion of the data subject into consideration and repeat the evaluation if necessary.

4. When the data subject objects to the processing of his personal data, the data controller must immediately cease the processing of personal data, except in cases provided by law, and inform the data recipients thereof.

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

6. At the request of the data subject, the data controller must store all the personal data of the data subject the processing whereof has ceased.

Article 20. Service to the Data Subject ➡

1. An institution authorised by the Government shall assist the data subject in exercising his right specified in Article 17 of this Law.

2. Upon applying to an institution authorised by the Government and submitting his identity document, the data subject may request the institution authorised by the Government 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 performing the function referred to in paragraph 2 of this Article, an institution

authorised by the Government 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 service specified in paragraph 2 of this Article shall be provided to the data subject for a certain fee. The fee shall not exceed the expenses of data collection and provision of the service. The Government or an institution authorised by it shall establish the amount of the fee.

CHAPTER IV. SECURITY OF DATA ➔

Article 21. Security of Data ➔

1. The data controller and data processor must implement appropriate organisational and technical measures, which would ensure the protection of personal data against any accidental or unlawful destruction, alteration, disclosure and 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.

2. 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. Upon authorising the data processor to process personal data, the data controller stipulates that personal data must be processed only on instructions from the data controller.

4. Only staff authorised by the data controller or data processor shall have the right to process personal data.

5. The staff processing personal data, when applying for a job or when performing their work, must assume an obligation, which must be in writing, to keep the personal data confidential when those data are not meant for public disclosure. This obligation shall remain valid after leaving the public service, transfer into another position or after the employment has ended.

CHAPTER V. REGISTRATION OF DATA CONTROLLERS ➔

Article 22. Notification of Data Processing ➔

1. The data controller may carry out automated processing of personal data subject to notification of the institution authorised by the Government in accordance with the procedure established by the Government, except when personal data are processed:

- 1) for the purposes of internal administration;
- 2) in cases specified in Article 5, paragraph 2, subparagraph 4;
- 3) in cases specified in Article 8;
- 4) in cases specified in Article 10;

5) following the procedure set forth in the Law of the Republic of Lithuania on State and Official Secrets.

Article 23. Registration of Data Controllers ➡

1. Data controllers shall be registered in the State Register of Personal Data Controllers which shall be established and its regulations shall be approved by the Government.
2. The State Register of Personal Data Controllers shall be administered by an institution authorised by the Government

CHAPTER VI. TRANSFER OF PERSONAL DATA TO DATA RECIPIENTS IN FOREIGN COUNTRIES ➡

Article 24. Transfer of Personal Data to Data Recipients in Foreign Countries ➡

1. Personal data shall be transferred to data recipients in foreign countries upon receiving an authorisation from the institution authorised by the Government, except in the cases referred to in paragraphs 4 and 5 of this Article.
2. The institution authorised by the Government shall issue an authorisation to transfer personal data to foreign countries, provided there is an adequate level of protection in these countries. The institution authorised by the Government shall assess the adequacy of the level of protection of personal data with account of the laws and other legislation in force in the foreign country to which the personal data are being transferred which ensure legal protection of personal data in accordance with the type of the data transferred, the methods, purposes and duration of the processing of data.
3. The institution authorised by the Government shall grant an authorisation to transfer personal data to a foreign country which cannot guarantee adequate level of legal protection of personal data on condition that the data controller providing personal data specifies in the contract the requirements for the safeguards of personal data to the recipient of the data.
4. Without an authorisation of the institution authorised by the Government personal data shall be transferred to a foreign country or an international law enforcement organisation only when:
 - 1) the data subject has given consent to the transfer of the data;
 - 2) the provision of personal data is necessary for the conclusion or performance of a contract between the data controller and a third party;
 - 3) the personal data are necessary for the performance of a contract which has been concluded by the data subject as one of the parties to the contract;
 - 4) the transfer of personal data is necessary in the interests of the State;
 - 5) the data are necessary for a court hearing;

6) for the purpose of protecting the life of the data subject;

7) it is necessary for the prevention or investigation of criminal offences.

5. Personal data may also be transferred without an authorisation of the institution authorised by the Government to foreign countries under international agreements to which the Republic of Lithuania is a party.

CHAPTER VII. MONITORING OF APPLICATION OF THIS LAW ➡

Article 25. Supervisory Authority ➡

1. The implementation of the Law on Legal Protection of Personal Data, with the exception of its Article 8, shall be supervised and monitored by the an institution authorised by the Government. The institution authorised by the Government shall be a government institution financed from the State budget. It shall be accountable to the Government. The regulations of the institution authorised by the Government shall be approved by the Government.

2. The institution authorised by the Government shall be guided by the Constitution of the Republic of Lithuania, laws, international agreements of the Republic of Lithuania, and, in discharging the functions established in this Law and taking decisions relating to the performance of the functions laid down in this Law, shall be independent: its rights may be restricted only by the law. The actions of the employees of the institution authorised by the Government relating to the performance of the functions laid down in this Law shall be appealed against only in the manner established by law.

Article 26. Functions of the Supervisory Authority ➡

The institution authorised by the Government 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 violations of personal data processing;

4) grant authorisations to data controllers to disclose personal data to data recipients in foreign countries;

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

6) draw up methodological recommendations on the protection of personal data and submit them to data controllers;

7) provide assistance, following the procedure established by law, to the 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 their administration.

Article 27. Rights of the Supervisory Authority ➔

1. The institution authorised by the Government shall be entitled:

1) to obtain free of charge all necessary information on the processing of personal data from data controllers, to access personal data that are being processed, and carry out inspections in places of processing of personal data in the cases provided by this Law;

2) to instruct data controllers on personal data processing and protection;

3) to draw up records about administrative offences in accordance with the procedure set forth in the Code of Administrative Offences;

4) to exchange information with personal data supervisory authorities in other countries to the extent that is necessary for the discharge of their duties;

5) to invite experts/consultants for examination of data processing or protection, as well as for drafting of documents on data protection;

6) to engage in legal proceedings where international and national law on personal data protection has been violated.

2. The institution authorised by the Government shall not have the right to control the processing of personal data in courts.

3. The employees of the institution authorised by the Government must keep secrecy of the personal data in respect of the confidential information to which they have access, and ensure its confidentiality, even after transfer to another position, leaving of the public service or after termination of their employment.

4. When drawing up rules/codes of conduct related to the processing of personal data, the data controllers and other persons must submit them to the opinion of the institution authorised by the Government.

5. The institution authorised by the Government must be notified if it is believed that the envisaged processing of personal data may threaten the rights of the data subject or may considerably damage the data (due to the type or volume of data, the number of data subjects, the purposes of data protection, the volume and frequency of disclosed data).

6. In the cases specified in paragraph 5 of this Article, the institution authorised by the Government shall carry out a prior check and give an opinion about the intended processing of personal data.

CHAPTER VIII. LIABILITY ➔

Article 28. Liability for Breaches of this Law ➔

Liability provided in the laws of the Republic of Lithuania shall apply to the data controllers, data processors and other persons who have violated this Law.

Article 29. Compensation for Material and Non-Material Damage ➡

1. Any person who has sustained damage as a result of unlawful processing of personal data or other acts or omissions by the data controller or data processor shall be entitled to claim compensation for material and non-material damage caused to him.
2. The court shall determine the extent of material and non-material damage.
3. The data controller, data processor or other person, after compensation for damage caused to the person, shall make a claim, in the manner established by law, for recovery of the loss sustained from the employee processing the data due to whose fault the loss occurred.