

LAW OF GEORGIA ON PERSONAL DATA PROTECTION

Chapter I General Provisions

Article 1. Purpose of the Law

The purpose of this Law is to ensure the protection of human rights and freedoms, including the protection of the right to privacy, in the course of the processing of personal data.

Article 2. Definition of terms

The terms used in this Law shall have the following meaning:

- a) **personal data** (hereinafter – data) – any information relating to an identified or identifiable natural person. An identifiable person is the one who can be identified directly or indirectly, in particular by reference to an identification number or to the factors specific to his/her physical, physiological, mental, economic, cultural or social identity;
- b) **special category of data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, state of health, sex life or conviction of a person, as well as biometric data which allow for a person’s identification through the above-mentioned factors;
- c) **biometric data** – any physical, mental or behavioral feature (fingerprints, iris scan, retina (retinal images), facial features and DNA), which is unique and permanent for each natural person and which can be used to identify this person;
- d) **processing of data** – any operation performed upon data, whether or not by automatic means, such as collection, recording, photographing, audio or video recording, organization, storage, alteration, restoration, consultation, use or disclosure by transmission, dissemination or otherwise making data available, alignment or combination, blocking, erasure or destruction;
- e) **automatic processing of data** – processing of data by means of information technologies;
- f) **data subject** – any natural person, regarding whom data are processed;
- g) **consent** — free consent of a data subject to the processing of data regarding him/her for a specific purpose, expressed orally, by means of telecommunication or other relevant means, which can clearly indicate the will of a data subject, after receiving relevant information by him/her;
- h) **written consent of a data subject** – free consent of a data subject to the processing of data regarding him/her for a specific purpose, signed or otherwise noted in writing or in an equivalent form by a data subject, after receiving relevant information by him/her;
- i) **data processor** – a public institution, natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data, processes personal data individually or with the help of an authorized person;
- j) **authorized person** – any natural or legal person, which processes data for or on behalf of a data processor;

- k) **data recipient** – a private or public institution, natural or legal person, employee of a private or public sector to whom data have been handed over, except for a personal data protection inspector;
- l) **third party** – any natural or legal person, public institution, other than a data subject, a personal data protection inspector, a data processor and an authorized person;
- m) **filing system** – a structured set of data, which are arranged and accessible according to specific criteria;
- n) **catalogue of a filing system** – a detailed description of the structure and content of a filing system;
- o) **register of the catalogues of filing systems** – a register that ensures a detailed registration of existing filing systems;
- p) **blocking of data** – temporal suspension of the processing of data;
- q) **depersonalization of data** – a type of modification of data that would make it impossible to link them with a data subject, or would require disproportionately huge efforts, costs and time to establish such a link;
- r) **identification number** – a personal identification number or any other identification number determined by the law and linked with a natural person, through which it would be possible to search or disclose data from a filing system (where an identification number is also processed);
- s) **personal data protection inspector** – an official responsible for the supervision over implementation of the data protection legislation;
- t) **direct marketing** – offering product, service, employment or temporary employment by means of mail, telephone call, e-mail or other means of telecommunication;

Article 3. Scope of application of the Law

1. This Law shall apply in the territory of Georgia to the processing of data wholly or partly by automatic means, as well as to the processing otherwise than by automatic means of data which form part of a filing system or are processed to form part of a filing system.
2. This Law shall also apply to:
 - a) processing of data by diplomatic missions and consular posts of Georgia abroad;
 - b) activities of a data processor, which is not registered in the territory of Georgia, but applies technical means present in Georgia for the processing of data, except for the cases when these technical means are applied for the transfer of data only. In such cases a data processor shall designate/determine a representative registered in Georgia.
3. This Law shall not apply to:
 - a) processing of data by a natural person for purely personal purposes, when the processing is not connected with his/her commercial or professional activities;
 - b) processing of data for case management purposes at the court;
 - c) processing of information which is considered state secret;
 - d) processing of data for the purposes of public and state security (including economic security), defense, operative-investigative activities and criminal investigation.
4. This Law (except for Article 17) shall not apply to the processing of data by media means for the purposes of informing the public, as well as to the processing of data for artistic and literature purposes.
5. Articles 19 and 20 of this Law shall not apply to the processing of data of its members by political parties, trade and other unions and religious organizations.

Article 4. Principles of the processing of data

The following principles shall be applied while the processing of data:

- a) data shall be processed fairly and lawfully, inflicting no damage to the dignity of a data subject;
- b) data shall be processed only for explicitly specified legitimate purposes;
- c) data shall be processed only to the extent necessary to achieve respective legitimate purposes. Data shall be adequate and not excessive in relation to the purposes for which they are processed;
- d) data shall be valid and accurate. False and inaccurate data shall be rectified, while the data which have been collected without legitimate grounds and the data which are incompatible with the processing purposes shall be blocked, erased or destroyed;
- e) data shall be kept only for as long as it is necessary for the processing of data purposes. After achieving the purpose for which data have been processed, they shall be blocked, erased or destroyed, or shall be kept in a form not leading to identification of a person, unless otherwise prescribed by the law.

**Chapter II
Rules on the Processing of Data**

Article 5. Grounds for the processing of data

The processing of data shall be permissible, if:

- a) data subject has given his/her consent;
- b) processing of data is envisaged by the law;
- c) processing of data is necessary for compliance with the obligations, compelled by the legislation, to which a data processor is subject;
- d) processing of data is necessary in order to protect the vital interests of a data subject;
- e) processing of data is necessary for the protection of legitimate interests of a data processor or a third party, except where such interests are overridden by the advanced interest of the protection of rights and freedoms of a data subject;
- f) according to the law, data are publicly accessible or a data subject has made them publicly accessible;
- g) processing of data is necessary for the protection of an important public interest, in accordance with the law;
- h) processing of data is necessary for the consideration of an application of a data subject (for providing service to him/her).

Article 6. Processing of special category of data

- 1. The processing of special category of data shall be prohibited.
- 2. The prohibition, envisaged by Paragraph 1 of this Article, shall not apply if:
 - a) data subject has given written consent to the processing of special category of data;
 - b) data subject has made the data regarding him/her public, without explicit prohibition of their usage;
 - c) processing of data is necessary for carrying out the employment obligations or enjoying the related rights by a data processor;

- d) processing of data is necessary for the protection of vital interests of a data subject or a third person and a data subject is physically or legally incapable of giving his/her consent to the processing of data;
 - e) data are processed for the purposes of the protection of public health, for the protection of a natural person's health by a medical institution (employee), also if this is necessary for the management or functioning of healthcare system;
 - f) data are processed in the course of conducting legitimate activities by a political, philosophical, religious or trade-union, association or other non-commercial organization. In such cases the processing of data can be related solely to the members of this organization or to the persons who have regular contact with this organization.
3. In the course of the processing of data on the basis of Sub-paragraph "f" of Paragraph 2 of this Article, disclosure of data to a third person without the consent of a data subject shall be prohibited.

Article 7. Protection of data on a diseased person

1. After the death of a data subject, the processing of data regarding him/her shall be allowed with the consent of a data subject's parent, child, grandchild or a spouse, or if 30 years have elapsed since the death of a data subject, except for the grounds envisaged by Articles 5 and 6 of this Law.
2. After the death of a data subject, the processing of data regarding him/her shall also be allowed, if it is necessary for realization of the rights to inheritance.
3. The processing of data on the grounds envisaged by Paragraphs 1 and 2 of this Article shall be prohibited, if a data subject has expressed in writing the will on the prohibition of the processing of data regarding him/her after death, except for the processing on the grounds envisaged by Articles 5 and 6 of this Law.
4. For the processing of a deceased person's name, sex, dates of birth and death, presence of the ground for the processing of data envisaged by this Law shall be not required.
5. The data on a deceased person can be disclosed for the historical, statistical and research purposes, except for the cases when a deceased person prohibited their disclosure in writing.

Article 8. Processing of data for the purposes of direct marketing

1. The data, received from publicly accessible sources, can be processed for the purposes of direct marketing.
2. Regardless of the purpose of the collecting of data, the following data can be processed for the purposes of direct marketing: name (names), address, telephone number, e-mail address, fax number.
3. On the basis of the consent of a data subject, issued in accordance with the rules established by this Law, any data can be processed for the purposes of direct marketing.
4. A data subject shall have the right to request in writing the termination of using the data regarding him/her for the purposes of direct marketing, to a data processor at any time.
5. A data processor shall be obliged to terminate the processing of data for the purposes of direct marketing within no later than 10 working days upon the receipt of a request of a data subject.
6. While the processing of data for the purposes of direct marketing, a data processor shall be obliged to notify a data subject on the right envisaged by Paragraph 4 of this Article.

Article 9. Processing of biometric data by a public institution

1. The processing of biometric data by a public institution shall be allowed only for the purposes of the security of persons and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts.
2. Regardless of the conditions envisaged by Paragraph 1 of this Article, the processing of biometric data shall be allowed in accordance with the rules established by the law, for the purposes of issuing an identity document or for identifying the person crossing the state border.

Article 10. Processing of biometric data by a private person

The processing of biometric data by a private person shall be allowed only if it is necessary for the purposes of conducting activities, for the security of persons and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts. Before using biometric data, a data processor shall notify a personal data protection inspector detailed information on the processing of biometric data, including the information notified to a data subject, the purpose of the processing of data and the safeguards of the protection of data, unless otherwise provided by the law.

Article 11. Video surveillance in the streets

1. Conducting video surveillance in the streets shall be allowed only for the purposes of crime prevention, as well as for the security of persons and protection of property, public order and the protection of minors from negative influence.
2. In case of installing a video surveillance system, public and private institutions shall be obliged to post a relevant warning sign in a visible place. In this case a data subject shall be considered to be informed on the processing of data regarding him/her.
3. A video surveillance system and recordings shall be protected from unlawful damage and use.

Article 12. Video surveillance of the buildings of public and private institutions

1. For the purposes of conducting proper monitoring, public and private institutions shall be allowed to conduct video surveillance of their buildings, if it is necessary for the purposes of the security of persons and protection of property, for the protection of minors from negative influence and the protection of secret information.
2. Only outdoor perimeter and entrance of a building can be monitored by a video surveillance system.
3. Installation of video surveillance system at the place of work can only be allowed in exceptional cases, if it is necessary for the purposes of the security of persons and protection of property, as well as for the protection of secret information, and if it is impossible to achieve these objectives by other means.
4. Conducting video surveillance in dressing rooms and the places of hygiene shall be prohibited.
5. All employees working in a relevant private or public institution shall be informed in writing about the video surveillance being conducted and of their rights.
6. A data processor shall be obliged to create a filing system, designed for storing video recordings. Except for recordings (photos/voice), a system should contain the information on the date, place and time of the processing of data.

Article 13. Video surveillance of a residential building

1. Installation of a video surveillance system in a residential building shall require a written consent of more than a half of the owners of this building.
2. Installation of a video surveillance system in a residential building shall be allowed only for the security purposes of persons and property.
3. Only the entrance and common space can be monitored by a video surveillance system, installed in a residential building. Monitoring of the apartments of owners shall be prohibited.
4. Monitoring of the entrance of an apartment by a video surveillance system shall be allowed only on the basis of a decision of the owner of this apartment or his/her written consent.

Article 14. Processing of data for the purposes of registering entries and exits from the buildings of public and private institutions

1. For the purposes of registering entries and exits from the buildings, public and private institutions can collect the following data: name, number and type of an identification document, address, dates and time of entries and exits, as well as purposes of entries and exits from the buildings.
2. The term of storage of the data envisaged by Paragraph 1 of this Article shall not exceed 3 years from the day of their registration, unless otherwise provided by the law. After the expiry of the three-year term, they shall be erased or destroyed.

**Chapter III
Rights and Obligations of a Data Processor and an Authorized Person**

Article 15. Supply of data to a data subject

1. If the collecting of data is conducted directly from a data subject, a data processor or an authorized person shall be obliged to supply a data subject with the following information:
 - a) identities and registered address of a data processor and of an authorized person (if applicable);
 - b) purpose of the processing of data;
 - c) whether the supply of data is obligatory or voluntary; if obligatory – the legal consequences of refusing;
 - d) right of a data subject to obtain information on the data processed regarding him/her, request their rectification, update, addition, blocking, erasure and destruction.
2. Supply of the information mentioned in Paragraph 1 of this Article shall not be obligatory, if a data subject already has it.
3. In case the collecting of data is not conducted directly from a data subject, a data processor or an authorized person shall be obliged to supply the information mentioned in Paragraph 1 of this Article to a data subject upon request.
4. While collecting information for the statistic, scientific and historic purposes, its supply shall not be obligatory, if the supply of information to a data subject involves disproportionately huge efforts.

Article 16. Processing of data by an authorized person

1. An authorized person can process data on the basis of a legal act or a written contract concluded with a data processor, which should be in compliance with the requirements established by this Law and other normative acts and should envisage the rules and restrictions established by this Law.
2. A data processor shall process data within the scope of a relative normative act or agreement. Any further processing of data by a data processor for any other purposes shall be prohibited. The transfer of the right to the processing of data to any other person by an authorized person, without the consent of a data processor, shall be prohibited.
3. Concluding an agreement on the processing of data shall be prohibited, if, due to the activities and/or purposes of an authorized person, there is the risk of the non-target processing of data.
4. A data processor shall make sure that an authorized person will apply appropriate organizational and technical measures for the protection of data. He/she shall be obliged to monitor the processing of data conducted by an authorized person.
5. In case of a dispute between an authorized person and a data processor, an authorized person shall be obliged to transfer the data available at him/her to a data processor, upon request.
6. In case of the termination of the activities by an authorized person, the data shall be immediately transferred to a data processor.
7. An obligation to apply measures for data security shall be envisaged in the agreement concluded with an authorized person.

Article 17. Data security

1. A data processor shall be obliged to apply the organizational and technical measures, which ensure the protection of data against accidental or unlawful destruction, alteration, disclosure, access, or any other form of unlawful use and accidental or unlawful loss.
2. A data processor shall be obliged to ensure the registration of all actions performed on electronic data. While the processing of non-electronic data, a data processor shall be obliged to register all actions on the disclosure and/or alteration of data.
3. The measures applied for data security shall be adequate to the risks related to the processing of data.
4. Any employee of a data processor and of an authorized person, who participates in the processing of data, shall be obliged not to exceed the scope of powers granted to him/her. Moreover, he/she shall be obliged to protect data security, even after the termination of the term of his/her office.
5. The measures on the protection of data security shall be defined by the Georgian legislation.

Article 18. Obligations of a data processor and of an authorized person on the disclosure of data

While the disclosure of data, a data processor and an authorized person shall be obliged to ensure the registration of the following information: which data is to be disclosed, to whom, when and on which legal grounds. This information shall be stored together with the data on a data subject, during the period of their storage.

Article 19. Catalogue of a filing system

1. A data processor shall be obliged to keep a catalogue of a filing system on each filing system and to register the following information:

- a) title of a filing system;
 - b) titles and address of a data processor and of an authorized person, place of storage and/or of processing of data;
 - c) legal grounds for the processing data;
 - d) category of a data subject;
 - e) category of data in a filing system;
 - f) purpose of the processing of data;
 - g) term of storage of data;
 - h) facts and grounds for restricting the rights of a data subject;
 - i) recipient of the data stored in a filing system and their categories;
 - j) information on the transfer of data to another state and international organization, and legal grounds for such transfer;
 - k) general description of the procedure established for the protection of data security.
2. A data processor shall be obliged to ensure regular update of the information envisaged by Paragraph 1 of this Article.

Article 20. Obligation to notify a personal data protection inspector

1. A data processor shall be obliged to notify in writing or by electronic means the information envisaged by Article 19 of this Law to a personal data protection inspector, before creating a filing system and before entering new category of data in it.
2. A data processor shall be obliged to notify a personal data protection inspector on making alterations to the information envisaged by Article 19 of this Law, no later than in 30 days from making the alteration.
3. A data processor, the number of employees of which does not exceed 20, shall be exempt from the fulfillment of the obligation envisaged by Paragraph 1 of this Article.

**Chapter IV
Rights of a Data Subject**

Article 21. Right of a data subject to request information

1. A data subject shall have the right to request information from a data processor on the processing of data regarding him/her. A data processor shall provide the following information to a data subject:
 - a) which information regarding him/her is being processed;
 - b) purpose of the processing of data;
 - c) legitimate grounds for the processing of data;
 - d) ways of collecting data;
 - e) persons to whom the data regarding him/her were issued, the grounds and purposes of issuance.
2. The supply of the data, envisaged by Sub-paragraph “e” of Paragraph 1 of this Article, to a data subject shall not be obligatory, if the data are made public, in accordance with the law.

3. A data subject shall receive the information, envisaged by Paragraph 1 of this Article, without delay, no later than in 10 days, from the day the request is made.
4. The form of submitting the information, envisaged by Paragraph 1 of this Article, shall be selected by a data subject.
5. A person shall have the right to check the personal data regarding him/her, stored in a public institution, and obtain the copies of these data free of charge, except for the data issuance of which requires fees in accordance with the Georgian legislation.

Article 22. Right of a data subject to request rectification, update, addition, blocking, erasure and destruction of data

1. In case a data subject requests, a data processor shall be obliged to rectify, update, add, block, erase or destroy data, if they are incomplete, inaccurate, outdated or they are collected and processed in violation of the law.
2. A data processor shall notify all data recipients about the rectification, updating, addition, blocking, erasure or destruction of data, except for the cases when the submission of such information is impossible due to the multiplicity of data recipients and disproportionately huge costs. A personal data protection inspector shall be notified about the latter circumstance.
3. In case of receiving information in accordance with Paragraph 2 of this Article, its recipient party shall be obliged to rectify, update, add, block, erase or destroy the data, accordingly.

Article 23. Procedures on rectification, updating, addition, blocking, erasure and destruction of data

1. The submission of a request, envisaged by Paragraph 1 of Article 22 of this Law, can be made in writing, orally or by electronic means.
2. A data processor shall be obliged to rectify, update, add, block, erase or destroy data or to notify a data subject of the grounds of the refusal, within 15 days of the receipt of the request of a data subject.
3. If a data processor independently, without the request of a data subject, considers that the data available to him/her are incomplete, inaccurate or outdated, he/she shall accordingly rectify or update the data and shall notify a data subject thereof.
4. After submitting the request, envisaged by Paragraph 1 of Article 22 of this Law, by a data subject, a data processor shall be authorized to block data on the basis of an applicant's request.
5. A decision on the blocking of data shall be made within 3 days from submitting a respective request and shall be in force until making a decision on the rectification, updating, addition, erasure and destruction of data.
6. A decision on the blocking of data shall be attached to respective data until the existence of the reason of blocking.

Article 24. Restriction of the right of a data subject

1. The rights of a data subject, envisaged by Articles 15, 21 and 22 of this Law, can be restricted by the Georgian legislation, if realization of these rights might threaten:
 - a) national security or defense interests of the country;
 - b) public security interests;
 - c) detection, investigation and prevention of crime;
 - d) important financial or economic interests of the country (including monetary, budgetary and taxation matters);

- e) rights and freedoms of a data subject and of others.
2. The measure, envisaged by Paragraph 1 of this Article, can be applied only to the extent necessary for achieving the purpose of the restriction.
3. In case the grounds envisaged by Paragraph 1 of this Article are present, a decision of a data processor or of a personal data protection inspector shall be notified to a data subject in a manner not to hinder the purpose of the restriction of the right.

Article 25. Objection to consent

1. A data subject shall have the right to refuse his/her prior consent at any time and without explanation and to request the termination of the processing of data and/or the destruction of the processed data.
2. A data processor shall be obliged to terminate the processing of data in accordance with the request of a data subject, and/or to destroy the processed data within 5 days from the submission of an application, if there are no other grounds for the processing of data.
3. This Article shall not apply to the information processed with the consent of a data subject, concerning the compliance with monetary obligations by him/her.

Article 26. Right to appeal

1. In case of violations of the rights envisaged by this Law, a data subject shall have the right to apply to a personal data protection inspector or to the court in accordance with the rules established by the law, but in case a data processor is a public institution, an application can also be submitted to the same or higher administrative organ.
2. A data subject shall have the right to request the blocking of data from the organ deciding upon the case, until rendering a decision.
3. A data subject shall have right to appeal the decision of a higher administrative organ or of a personal data protection inspector to the court, in accordance with the rules established by the law.
4. In case a dispute arises concerning the existence of the consent of a data subject on the processing of data, a data processor shall bear the burden of prove regarding the existence of the fact of the consent of a data subject.

Chapter V
Personal Data Protection Inspector

Article 27. Basic purposes of the activities of a personal data protection inspector

1. A personal data protection inspector (hereafter - inspector) shall be responsible for monitoring the legality of the processing of data in Georgia. The main purposes of the activities of a personal data protection inspector shall be:
 - l) to provide consultations with public and private institutions (persons) on matters related to the data protection;
 - m) to consider applications on the data protection;
 - n) to examine (to inspect) the lawfulness of the processing of data in public and private institutions;

- o) to inform the public about the situation concerning the protection of data and important developments related thereto in Georgia;
2. The terms of activities of an inspector and of exercising his/her powers shall be defined by a statute to be approved by the Government of Georgia.

Article 28. Appointment and termination of the term of office of an inspector

1. An inspector shall be appointed through the open competition procedure.
2. The Prime Minister of Georgia shall establish a competition commission for the selection of an inspector. The commission shall include the representatives of the Government of Georgia, of the Parliament of Georgia, of the judicial authority, of the Office of the Public Defender of Georgia, as well as of the non-governmental sector, on the basis of the principle of proportionality.
3. An inspector shall be a citizen of Georgia, who has relevant high education, relevant professional experience, and possesses professional and moral qualities which enable him/her to perform the functions of an inspector.
4. A competition commission for the selection of an inspector shall select a candidate of an inspector by the majority of votes and shall present him/her to the Prime Minister of Georgia for the appointment.
5. The Prime Minister shall appoint an inspector within 10 days, or shall announce a new competition.
6. An inspector shall be appointed for the term of 3 years. The same person can be appointed as an inspector for 2 consecutive terms only.
7. An inspector shall be selected no earlier than 60 days prior to the expiry of the term of office of the incumbent and no later than 30 days after the expiry of his/her term of office.
8. The term of office of a newly-appointed inspector shall commence on the day following the expiry of the term of office of the incumbent in case he/she was appointed before the expiry of this term, or on the day following the appointment – in case he/she was appointed after the expiry of this term or in case the incumbent's term was prematurely terminated.
9. The term of office of an inspector shall be terminated upon the expiry of 3 years from the appointment or upon the premature termination thereof.
10. An inspector shall have a deputy, appointed by an inspector.

Article 29. Incompatibility with the office of an inspector

1. The office of an inspector shall be incompatible with the membership of the state and local self-government representative bodies of Georgia, with holding any public office and being engaged in remunerated activities, other than scientific, pedagogic and artistic activities. He/she cannot be a member of a political party and shall be restricted from participating in political activities.
2. Within 1 month from the selection, an inspector shall be obliged to terminate activities incompatible with his/her office. If an inspector fails to comply with the above requirement within the mentioned term, his/her term of office shall be terminated and a competition commission for the selection of an inspector shall present a new candidate of an inspector to the Prime-Minister of Georgia.

Article 30. Premature termination of the term of office of an inspector

1. The term of office of an inspector shall be prematurely terminated, if:
 - a) he/she loses citizenship;

- b) he/she is unable to perform his/her obligations for 4 consecutive months;
 - c) court judgment of conviction against him/her enters into force;
 - d) court finds him/her lacking legal capacity, recognizes missing or declares deceased;
 - e) he/she has accepted or holds the post incompatible with the office of an inspector or conducts the activities incompatible with his/her office;
 - f) he/she resigns;
 - g) he/she dies.
2. In the cases envisaged by Paragraph 1 of this Article, the term of office of an inspector shall be considered to be terminated from the moment any of the above-mentioned grounds are established. This shall be notified to the Prime Minister of Georgia without delay. The Prime Minister of Georgia shall issue a respective administrative-legal act on the termination of the term of office of an inspector.
3. In the cases envisaged by Paragraphs “b” and “e” of Paragraph 1 of this Article, the term of office of an inspector shall be terminated by the decision of the Prime Minister of Georgia.
4. In case of the premature termination of the term of office of an inspector and before the selection of a new inspector by the competition commission for the selection of an inspector, a deputy inspector shall carry out his/her obligations, and shall be subject to the rights and legal safeguards granted to an inspector.

Article 31. Independence of an inspector

1. In exercising his/her powers an inspector shall be independent and shall not be subordinated to any other public official or body. An inspector shall be guided by the Constitution of Georgia, international agreements, this Law, other normative acts and a statute. Any influence or interference with an inspector’s activities shall be prohibited and punished by the law.
2. For ensuring the independence of an inspector, the state shall be obliged to provide him/her with appropriate working conditions.
3. An inspector shall have the right not to testify concerning the fact confided to him/her as to an inspector. This right shall be preserved to him/her even after the termination of the term of office.

Article 32. Financial and organizational support to the activities of an inspector

1. An inspector shall enjoy his/her rights and carry out his/her obligations with the support of an inspector’s office (hereinafter – office).
2. The structure of the office, rules of activities and of division of powers among the employees shall be established by a statute of the office.
3. The office shall be managed directly by an inspector or by a deputy of an inspector on his/her instructions.
4. Activities of an inspector and of the office shall be financed from the state budget of Georgia. An inspector shall present a draft expenditure plan in accordance with the rules established by the law. The banknotes necessary for the activities of an inspector and of the office shall be defined by a separate code of the state budget of Georgia.
5. For the implementation of the rights and obligations envisaged by this Law, an inspector shall be authorized to receive grants and contributions in accordance with the rules established by the Georgian legislation.

Article 33. Providing consultations and conducting educational activities

1. In case of a relevant request an inspector shall be obliged to provide consultations to the state and local self-government bodies of Georgia, other public institutions, legal persons of private law and natural persons on any matter related to the processing and protection of data.
2. An inspector shall conduct educational activities on the matters related to the processing and protection of data.

Article 34. Consideration of an application of a data subject by an inspector

1. An inspector shall be obliged to consider an application of a data subject on the processing of data and to apply the measures envisaged by this Law.
2. Within 10 days from the adoption of an application, an inspector shall make a decision on the measures to be taken and shall notify an applicant thereof.
3. An inspector shall be authorized to conduct an examination for the purposes of studying and analyzing the circumstances related to the application. In case of an inspector's request, a data processor and an authorized person shall be obliged to supply him/her with relevant information and documents.
4. Time for the consideration of an application of a data subject by an inspector shall not exceed 2 months. Time for the consideration of an application can be prolonged by no more than 1 month on the basis of a grounded decision of an inspector.
5. Until the completion of the consideration of an application of a data subject, an inspector shall be authorized to make a decision on the blocking of data. Regardless of the blocking of data, the processing of these data can be prolonged if it is necessary for the protection of the vital interests of a data subject or a third person, as well as for the purposes of state security and defense.
6. After the consideration of an application of a data subject, an inspector shall make a decision on the application of one of the measures envisaged by Article 39 of this Law, what shall be notified to a data subject and a data processor without delay.

Article 35. Examination conducted by an inspector

1. An inspector shall be authorized to conduct an examination of any data processor and authorized person, based on his/her own initiative as well as on the statement of an interested person.
2. Examination conducted by an inspector shall imply:
 - a) establishing of the protection of the principles on the processing of data and of the existence of the legitimate grounds for the processing of data;
 - b) examining the compatibility of the applied procedures and organizational and technical measures in accordance with the requirements established by this Law;
 - c) examining the compliance of the requirements established by this Law concerning a catalogue of filing system, register of the catalogues of filing systems and registration of data issuance;
 - d) examining the lawfulness of the transmission of data to other states and international organizations;
 - e) examining the compliance with the rules related to the protection of data, established by this Law and other normative acts.
3. In the course of examination an inspector shall be authorized to request documents and information necessary for conducting an examination within the scope established by Paragraph 2 of this Article, from any institution, natural and legal persons.
4. A data processor and an authorized person shall be obliged to submit any information and document to an inspector without delay. If this is impossible due to physical or legal reasons, they can submit information or documents to an inspector no later than 15 days from the request.

5. An inspector shall be authorized to enter any institution and organization for the purposes of conducting an examination, and check any document and information, regardless of their content and the way they are stored, except for the cases envisaged by Paragraph 6 of this Article.
6. An inspector shall be obliged to give a prior notification, at least 3 days in advance, on the planned examination and its scope, to the institution, activities of which are related to the state security and defense or which conducts operative-investigative activities.
7. Considering the results of an examination, an inspector shall be authorized to apply the measures envisaged by Article 39 of this Law.
8. An inspector, his/her deputy and the employees of the office shall be obliged not to disclose or conduct any unlawful processing of the information, which has been revealed to them in the course of examination or as a result of any other kind of official activities.

Article 36. Participation of an inspector in the law-making process

An inspector shall be authorized to submit proposals to the Parliament of Georgia and other public institutions for the purposes of the improvement of the legislation and prepare conclusions on the laws and other normative acts related to the processing of data, on his/her own initiative.

Article 37. Cooperation of an inspector with other organizations and institutions

An inspector shall be authorized to cooperate with other institutions, international organizations and relevant institutions of other states on any matter related to the protection of data.

Article 38. Annual report of an inspector

1. An inspector shall submit a report to the Government of Georgia once a year, on the situation concerning the protection of data in the country. An inspector's report shall be made public and an inspector shall ensure its publication.
2. An inspector's report shall include general assessment of the situation concerning the protection of data, conclusions and recommendations, as well as the information on important violations identified during a year and the measures undertaken.

Article 39. Measures applied by an inspector for the implementation of the law

1. If an inspector identifies a violation of this Law or other normative acts regulating the processing of data, he/she shall be authorized:
 - a) to require the eradication of the violation and the deficiencies related to the processing of data in the form and within the term indicated by him/her;
 - b) to require the temporary or permanent termination of the processing of data, if the measures and procedures applied by a data processor or an authorized person for the safety of data, does not comply with the requirements of the law;
 - c) to demand the termination of the processing of data, their blocking, erasure, destruction or depersonalization, if he/she considers that the processing of data is conducted unlawfully;
 - d) to demand the termination of the transfer of data to another state and international organization, if their transfer is conducted in violation of the requirements of this Law;

- e) to give written advices and provide recommendations to a data processor and an authorized person, in case of minor violations of the rules on the processing of data by them.
2. A data processor and an authorized person shall be obliged to comply with the requirements of an inspector in the term indicated by him/her and notify an inspector thereof.
3. An inspector shall be authorized to address the court, if a data processor or an authorized person does not comply with the requirements of an inspector.
4. If an inspector reveals an administrative offence, he/she shall be authorized to draw up an administrative offence protocol and respectively impose administrative liability on a data processor or an authorized person, in accordance with the rules established by the law.
5. If an inspector considers in the course of activities that the elements of crime are present, he/she shall be obliged to notify this to a competent state authority, in accordance with the rules established by the law.
6. An inspector's decision shall be obligatory to be implemented and it shall be appealed only to the court, in accordance with the rules established by the law.

Article 40. Register of the catalogues of filing systems

1. An inspector shall be obliged to keep a register of the catalogues of filing systems, which shall contain the information envisaged in Paragraph 1 of Article 19 of this Law.
2. The information contained in the register of the catalogues of filing systems shall be made public and an inspector shall ensure its proper publication.

Chapter VI
Transfer of Data to Other States and International Organizations

Article 41. Transfer of data to another state and international organization

1. Transfer of data to another state and international organization shall be allowed, if the grounds for the processing of data envisaged by this Law are present and if adequate safeguards for the protection of data are ensured in a respective state or international organization.
2. Transfer of data to another state and international organization, except for Paragraph 1 of this Article, shall also be allowed, if:
 - a) transfer of data is envisaged by an international agreement of Georgia;
 - b) data processor provides adequate safeguards for the protection of data and the protection of the fundamental rights of a data subject on the basis of an agreement concluded between a data processor and a respective state, a natural or legal person of that state or an international organization.
3. Transfer of data on the basis of Sub-paragraph "b" of Paragraph 2 of this Article shall be allowed only after the permission of an inspector.

Article 42. Establishing adequate safeguards for the protection of data

Presence of adequate safeguards for the protection of data in a foreign state and/or in an international organization shall be assessed and decided upon by an inspector, on the basis of an analysis of the processing of data legislation and practice.

Chapter VII

Administrative Liability for Violations of This Law

Article 43. Processing of data in the absence of the grounds envisaged by this Law

1. The processing of data in the absence of the grounds envisaged by this Law - shall entail a warning or a fine in the amount of GEL 500.
2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year – shall entail a fine in the amount of GEL 2000.

Article 44. Violation of the principles of the processing of data

1. Violation of the principles of the processing of data envisaged by this Law - shall result in a warning or a fine in the amount of GEL 500.
2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year – shall result in a fine in the amount of GEL 2000.

Article 45. Processing of special category of data in the absence of the grounds envisaged by this Law

1. The processing of special category of data in the absence of the grounds envisaged by this Law – shall result in a fine in the amount of GEL 1000.
2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year – shall result in a fine in the amount of GEL 5000.

Article 46. Failure to comply with the requirements on data security

1. Failure to comply with the requirements established by this Law on data security - shall result in a warning or a fine in the amount of GEL 500.
2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year –

shall result in a fine in the amount of GEL 2000.

Article 47. Violation of the rules on using data for the direct marketing purposes

1. Using of data for the direct marketing purposes in violation of the rules established by this Law - shall result in a fine in the amount of GEL 3000.

2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year – shall result in a fine in the amount of GEL 10000.

Article 48. Violation of the rules on video surveillance

1. Violation of the rules on video surveillance, established by this Law - shall result in a warning or a fine in the amount of GEL 500.

2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year – shall result in a fine in the amount of GEL 2000.

Article 49. Violation of the rules on the processing of data regarding entries and exits from the buildings of public and private institutions

Violation of the rules, established by this Law, on the processing of data regarding entries and exits from the buildings of public and private institutions -

shall result in a warning or a fine in the amount of GEL 100.

Article 50. Violation of the rules on notification of a data subject by a data processor

1. Violation of the rules, established by this Law, on notification of a data subject by a data processor - shall result in a warning or a fine in the amount of GEL 100.

2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year – shall result in a fine in the amount of GEL 500.

Article 51. Giving assignment by a data processor to the person authorized to process data in violation of the rules

1. Giving assignment by a data processor to the person authorized to process data in violation of the rules established by this Law - shall result in a fine in the amount of GEL 500.

2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year –

shall result in a fine in the amount of GEL 2000.

Article 52. Violation of the rules envisaged by Article 16 of this Law by an authorized person

1. Violation of the rules, envisaged by Article 16 of this Law, by an authorized person - shall result in a fine in the amount of GEL 1000.
2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year , - shall result in a fine in the amount of GEL 3000.

Article 53. Failure to comply with the requirements of an inspector

1. Violation of the rules on submitting information and documents to an inspector or to a person authorized by him/her, by a data processor or by an authorized person - shall result in a warning or a fine in the amount of GEL 500.
2. The same act committed by the person, subjected to an administrative penalty for the violation envisaged by Paragraph 1 of this Article during 1 year, - shall result in a fine in the amount of GEL 2000.

Article 54. Violation of other rules on the processing of data

Violation of the rules established by this Law, except for the actions envisaged by Articles 43-53 of this Law, - shall result in a warning or a fine in the amount of GEL 100.

Article 55. Reviewing the case of administrative offence

1. An inspector shall have the right to review the cases of administrative offences, envisaged in Articles 43-54 of this Law, and to impose relevant administrative sanctions.
2. An inspector shall be authorized to draw up an administrative offence protocol.
3. A person authorized by an inspector draws up an administrative offence protocol and reviews the case in accordance with the rules established by the Code of Administrative Offences of Georgia.

**Chapter VIII
Transitional Provisions**

Article 56. Entry into force of the Law

1. This Law, except for Articles 43-55 of this Law, shall enter into force on 1 May 2012.
2. Articles 43-55 of this Law shall enter into force on 1 January 2013.
3. Articles 34, 35 and 39 of this Law shall enter into force with regard to the private sector on 1 January 2016.

President of Georgia
Tbilisi,
December 28, 2011
#5669-RS

Mikhail Saakashvili