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 fundamental human rights and freedoms, including the right to the inviolability of private and family life, and to privacy and communication, in the processing of personal data.

Article 2 – Scope of the Law
1. This Law shall apply to the processing of data wholly or partly by automated means within the territory of Georgia, to the processing other than by automated means of data which form part of a filing system or are processed to form part of a filing system, as well as to the processing of data by a controller not established in Georgia, using technical means available in Georgia, except where the technical means are used solely for the transit of data.
2. This Law shall not apply to:
a) the processing of data by a natural person in the course of purely personal and/or household activities, which has no connection to his/her entrepreneurial and/or economic and professional activities or the performance of official duties. The processing of data in the course of purely personal and/or household activities can include correspondence and the holding of addresses, or online activity (including social networking) undertaken within the context of such activities;
b) the processing of data for the purposes of national security (including economic security), defence, intelligence and counter-intelligence activities;
c) semi-automated processing and non-automated processing of data deemed to be a state secret, for the purposes of the prevention, investigation and prosecution of crime, and the conduct of operative and investigative activities or the protection of the rule of law;
d) the processing of data for the purposes of court proceedings;
e) the processing of data by mass media for public information (except for Article 4(1)(f) and Article 27);
f) the processing of data for academic, artistic or literary purposes.
4. Article 6 of this Law shall not apply to the processing of data for the purposes of a population census as provided for by the Law of Georgia on Official Statistics.
4. This Law shall apply to the automated and semi-automated processing of data by institutions that carry out the activities under Article 2(b-d), and to the non-automated processing of data which form part of a filing system or are processed to form part of a filing system, unless the data are processed in the context of the activities under the same subparagraphs.
5. Anyone who unknowingly obtains another person's data that is not intended for him/her shall respect the rights of the data subject and shall not attempt to carry out unlawful data processing.

Article 3 – Definition of terms
For the purposes of this Law, the terms used herein shall have the following meanings:
a) personal data ('data') – any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, including by his/her name, surname, identification number, location data and electronic communication identifiers, or by physical, physiological, mental, psychological, genetic, economic, cultural or social characteristics;
b) special categories of data – data connected to a person's racial or ethnic origin, political views, religious, philosophical or other beliefs, membership of professional unions, health, sexual life, status of an accused, convicted or acquitted person or a victim in criminal proceedings, conviction, criminal record, diversion, recognition as a victim of trafficking in human beings or of a crime under the Law of Georgia on the Elimination of Violence against Women and/or Domestic Violence, and the Protection and Support of Victims of Such Violence, detention and enforcement of his/her sentence, or his/her biometric and genetic data that are processed to allow for the unique identification of a natural person;
c) data concerning health – data related to the physical or mental health of a data subject, including the provision of health care services, which reveal information about his/her physical or mental health;
d) biometric data – data processed using technical means and related to the physical, physiological or behavioural characteristics of a data subject (such as facial images, voice characteristics or dactyloscopic data), which allow the unique identification or confirm the identity of that data subject;
e) genetic data – data relating to the acquired or inherited genetic characteristics of a data subject which, through an analysis of a biological sample from that data subject, give unique information about his/her physiology or health;
f) processing of data – any operation performed on personal data, including collecting, obtaining, accessing, photographing, video monitoring and/or audio monitoring, organising, grouping, interconnecting, storing, altering,

retrieving, requesting for access, using, blocking, erasing or destroying, and disclosing by transmission, publication, dissemination or otherwise making available;
g) automated data processing – the processing of data by means of information technologies;
h) non-automated data processing – the processing of data without using information technologies;
i) semi-automated data processing – the processing of data without using information technologies;
j) filing system – a structured set of data which are arranged and accessible according to specific criteria;
k) data subject – any natural person whose data are being processed;
l) consent of the data subject – consent freely and unambiguously expressed by a data subject after the receipt of the respective information, by an active action, in writing (including in electronic form) or verbally, to the processing of data concerning him/her for specific purposes;
m) written consent of the data subject – consent, signed or otherwise expressed by a data subject in writing (including in electronic form) after the receipt of the respective information, to the processing of data concerning him/her for specific purposes;
n) controller – a natural person, a legal person, or a public institution, who individually or in collaboration with others determines the purposes and means of the processing of data, and who directly or through a processor processes data;
o) joint controllers – two or more controllers who jointly determine the purposes and means of data processing;
p) processor – a natural person, a legal person, or a public institution, which processes data for or on behalf of the controller. A natural person who is in labour relations with the controller shall not be considered a processor;
q) recipient – a natural person, a legal person, or a public institution, to which data are disclosed, except the Personal Data Protection Service;
r) categories of recipients – the classification/grouping of recipients according to their area of activities or organisational and legal form;
s) third party – a natural person, a legal person, or a public institution, other than a data subject, the Personal Data Protection Service, a controller, a processor, a special representative and persons who, under the direct authority of the controller or processor, are authorised to process data;
t) special representative – a natural or legal person established outside Georgia, or an association of persons with no legal personality, designated/appointed by the controller or processor as a representative on the basis of this Law;
u) personal data protection officer – a person designated/appointed by a controller or a processor, who performs the functions as provided for by Article 33 of this Law;
v) blocking of data – the temporary suspension of data processing (except storing);
w) video monitoring – the processing of visual image data using the technical means located/installed in a public or private space, including video control and/or video recording (except for covert investigative actions);
x) audio monitoring – the processing of audio signal data using the technical means located/installed in a public or private space, including audio control and/or audio recording (except for covert investigative actions);
y) direct marketing – the direct and immediate delivery of information to a data subject by telephone, mail, email or other electronic means to generate and maintain interest in, sell and/or support a natural and/or legal person, product, idea, service, work and/or initiative, as well as image and social issues. The provision of information by a public institution to a natural person shall not be considered direct marketing if the provision of such information is compatible with any of the grounds for data processing as provided for by Articles 5 and 6 of this Law;
z) profiling – any form of automated processing of data involving the use of data to evaluate certain personal characteristics relating to a natural person, in particular to analyse or predict characteristics concerning the natural person's performance of work, his/her economic situation, health, personal interests, reliability, behaviour, location or movements;
z_1) data depersonalisation – the processing of data in such a manner that the data cannot be attributed to the data subject or attributing them to the data subject involves disproportionate effort, expense and/or time;
z_2) data pseudonymisation – the processing of data in such a manner that the data cannot be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and, by virtue of technical and organisational measures, the data are not attributed to an identified or identifiable natural person;
z_3) incident – breach of security of data leading to the unlawful or accidental damage or loss of data, or the unauthorised disclosure, destruction, alteration of or access to data, or the collection/obtaining of data, or other unauthorised processing;
z_4) public institution – an institution as defined in Article 27(a) of the General Administrative Code of Georgia (except for political and religious associations);
z_5) continuing offence – an offence as provided for by this Law, the commission of which starts with an act and which then is committed continuously. A continuing offence shall be considered completed upon the termination of the act;
z_6) covert investigative action – an investigative action as provided for by Article 143^1(1) of the Criminal Procedure Code of Georgia;
z) the Agency – the Legal Entity under Public Law called the Operative-Technical Agency of Georgia, a body with

exclusive authority to conduct covert investigative actions as provided for by Article 143^1(1)(a-d) of the Criminal Procedure Code of Georgia;

z_8) electronic control system – the system as provided for by Article 2(i) of the Law of Georgia on the Legal Entity under Public Law called the Operative-Technical Agency of Georgia;

z_9) special electronic control system – the system as provided for by Article 2(j) of the Law of Georgia on the Legal Entity under Public Law called the Operative-Technical Agency of Georgia;

z_{10}) electronic control system of the central bank of electronic communication identification data – the system as provided for by Article 2(k) of the Law of Georgia on the Legal Entity under Public Law called the Operative-Technical Agency of Georgia;

z_{11}) special electronic control system for real-time location – the system as provided for by Article 2(n) of the Law of Georgia on the Legal Entity under Public Law called the Operative-Technical Agency of Georgia.

Chapter II – Lawfulness of Data Processing

Article 4 – Principles of data processing

1. The following principles shall be observed during data processing:

a) data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). The obligation to ensure the transparency of data processing shall not apply to the exceptional cases established by this Law;

b) data shall be collected/obtained for specified, explicit and legitimate purposes. The further processing of data for other purposes that are incompatible with the initial purposes shall be inadmissible;

c) data shall be processed only to the extent necessary to achieve the respective legitimate purpose. The data shall be proportionate to the purpose for which they are processed;

d) data shall be valid and accurate and, where necessary, kept up to date. Having regard to the purposes of data processing, inaccurate data shall be rectified, erased or destroyed without undue delay;

e) data may be stored only for a period which is necessary for achieving the legitimate purpose for which the data are processed. Once the purpose for which the data was processed has been achieved, the data shall be erased, destroyed or stored in a depersonalised form, unless the processing of data is required by law and/or a subordinate normative legal act issued in accordance with law, and the storing of data is a necessary and proportionate measure in a democratic society to safeguard overriding interests;

f) to ensure the security of data, technical and organisational measures shall be taken during the processing of data to ensure appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction and/or damage.

2. If data are to be processed for purposes other than those for which they have been collected/obtained, and the processing is not based on the consent of the data subject or on law, the controller shall, in order to decide whether the data were processed for purposes other than those for which they have been collected/obtained, take into account:

a) any link between the initial purpose for which the data have been collected/obtained and the intended further purpose;

b) the nature of the relationship between the controller and the data subject in the context of collecting/obtaining data;

c) whether the data subject has reasonable expectations as to the further processing of data concerning him/her;

d) whether special categories of data are processed;

e) possible consequences for the data subject that may accompany further data processing;

f) the existence of technical and organisational safeguards.

4. Data collected by a law enforcement agency in the course of its activities may be processed for the purpose of general analysis of criminal activity and to establish the relationship between the various offences detected.

4. For the purposes of observing the principle of data processing under paragraph 1(d) of this article, the controller shall ensure that, depending on the context, data based on facts are distinguished from data based on personal assessments. In the case of data based on personal assessments, strict compliance with the principle of data processing under paragraph 1(d) of this article is not mandatory.

5. The further processing of data by the controller for the purposes of crime prevention (including the conduct of appropriate analytical research), investigation, prosecution, the administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences and probation, ensuring the placement of a person in a temporary detention cell, combating illegal migration, the implementation of international protection, responding to administrative offences, ensuring public and fire safety, the conduct of operative and investigative activities, the safeguarding of public safety and/or the protection of the rule of law (including the conduct of criminological research by a relevant law enforcement body or a court), shall not be considered to be incompatible with initial purposes if the processing of data is required by law, or a law and a subordinate normative act issued on the basis thereof.

6. The further processing of data for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes shall not be considered to be incompatible with initial purposes. Long-term storage of data for the purposes referred to in this paragraph shall be permitted if appropriate technical and organisational measures are in place to protect the rights of the data subject.
7. The controller shall be responsible for, and demonstrate compliance with, the principles under this article when processing data.

Article 5 – Grounds for data processing

1. Data processing shall be admissible where one of the following grounds exists:
a) the data subject has given consent to the processing of data concerning him/her for one or more specific purposes;
b) data processing is necessary for the performance of a contract entered into with the data subject or to enter into a contract at the request of the data subject;
c) data processing is provided for by law;
d) data processing is necessary for the controller to perform his/her statutory duties;
e) according to law, the data are publicly available or the data subject has made them publicly available;
f) data processing is necessary to protect the vital interests of the data subject or another person, including to monitor epidemics and/or prevent their spread, or manage humanitarian crises and natural and man-made disasters;
g) data processing is necessary to protect substantial public interests;
h) data processing is necessary to perform tasks falling within the scope of public interest as defined by the legislation of Georgia, including for the purposes of crime prevention, investigation, prosecution, the administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences and probation, the conduct of operative and investigative activities, the safeguarding of public safety and/or the protection of the rule of law, including information security and cyber security;
i) data processing is necessary to protect important legitimate interests pursued by the controller or a third party, unless there is an overriding interest in protecting the rights of the data subject (including a minor);
j) data processing is necessary to review an application submitted by the data subject (to provide services to him/her).
2. The controller shall have an obligation to justify the legal basis for the processing of data.

Article 6 – Processing of special categories of data

1. The processing of special categories of data shall be permitted only if the controller provides safeguards for the rights and interests of the data subject as provided for by this Law and if one of the following grounds exists:
a) the data subject has given consent to the processing of the special category data for one or more specified purposes;
b) the processing of special categories of data is expressly and specifically regulated by law, and their processing is a necessary and proportionate measure in a democratic society;
c) the processing of special categories of data is necessary to protect the vital interests of the data subject or another person and the data subject is physically or legally incapable of giving consent to the processing of special categories of data;
d) the processing of special categories of data is necessary in the area of health care for the purposes of preventive, prophylactic, diagnostic, therapeutic, rehabilitative and palliative care, and for the management of services, medical equipment and the quality and safety of products, public health and the health care system, in accordance with the legislation of Georgia or a contract with a health professional (if these data are processed by a person who has an obligation to protect professional secrets);
e) the processing of special categories of data is necessary for the purposes of performing the statutory duties of the controller or exercising the specific rights of the data subject in the field of social security and social protection, including for the management of the social security system and services;
f) the processing of special categories of data is necessary for the purposes of crime prevention (including the conduct of appropriate analytical research), investigation, prosecution, the administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences and probation, ensuring the placement of a person in a temporary detention cell, combating illegal migration, the implementation of international protection, responding to administrative offences, ensuring public and fire safety, the conduct of operative and investigative activities, the safeguarding of public safety and/or the protection of the rule of law (including the conduct of criminological research by a relevant law enforcement body or a court), and the processing of such data is required by law, or a law and a subordinate normative act issued on the basis thereof;
g) special categories of data are processed to ensure information security and cyber security;
h) the processing of special categories of data is necessary because of the nature of labour obligations and relations, including for making decisions on employment and assessing the working capacity of the employee;
i) the data subject has made his/her data publicly available without an explicit prohibition of their use;
j) the processing of special categories of data is necessary to protect substantial public interests;
k) special categories of data are processed by political or professional associations, and organisations with religious or non-religious philosophical aims, for their legitimate activities. In this case, the processing of such data may relate solely to the members or former members of this association/organisation or persons who have regular contact with this

association/organisation in connection with its purposes, on condition that these data are not disclosed to a third party without the consent of the data subjects;
l) the processing of special categories of data is necessary for archiving purposes in the public interest as provided for by law, for scientific or historical research purposes or statistical purposes if the law provides for the implementation of appropriate and specific measures to protect the rights and interests of the data subject. This ground for the processing of special categories data shall not apply if a special law expressly provides for the restriction of the processing of such data under additional and different conditions;
m) special categories of data are processed for the purpose of the functioning of the Unified Migration Analytical System;
n) special categories of data are processed for the purposes of exercising the right to education of persons with disabilities and persons with special educational needs;
o) special categories of data are processed for the purposes of reviewing the issue under Article 11(2) of the Law of Georgia on the Elimination of Violence against Women and/or Domestic Violence, and the Protection and Support of Victims of Such Violence;
p) special categories of data are processed for the purpose of the re-socialisation and rehabilitation of convicted persons and former prisoners, and for the coordination of the process of the referral of minors;
q) special categories of data are processed for the purposes of issuing and publishing as public information, in accordance with the Organic Law of Georgia on General Courts, a judicial act adopted as a result of open court hearings;
r) special categories of data are processed in cases expressly provided for by the Law of Georgia on Public Procurement;
s) special categories of data are processed for the functioning of the institutional inter-agency coordination mechanism – for the purposes of identifying and/or managing cases involving harm or anticipated risks to the life, health or safety of the child and/or to the best interests of the child or to his/her rights, and ensuring, within the limits of these purposes, coordination between competent bodies (agencies) as designated by the Government of Georgia in the cases provided for by Article 83(3) and Article 84(2^1) of the Code on the Rights of the Child.
2. In the case of the processing of data as provided for by paragraph 1(q) of this article, they may be issued and published as public information in accordance with the Organic Law of Georgia on General Courts.
3. The controller shall have an obligation to justify the legal basis for the processing of special categories of data.

Article 7 – Procedure and conditions for giving consent to the processing of data relating to a minor

1. The processing of data relating to a minor shall be permitted on the basis of his/her consent if he/she has attained the age of 16, and the processing of data relating to a minor under the age of 16 shall be permitted with the consent of his/her parent or other legal representative, except in cases expressly provided for by law, including where the consent of a minor between the ages of 16 and 18 and his/her parent or other legal representative is required for the processing of data.
2. The controller shall be obliged to take reasonable and adequate measures to confirm the existence of the consent of the parent or other legal representative of a minor under the age of 16.
3. The processing of special categories of data relating to a minor shall be permitted only on the basis of the written consent of the minor's parent or other legal representative, except in cases expressly provided for by law.
4. When processing data relating to a minor, the controller shall be obliged to take into account and protect the best interests of the minor.
5. The consent of a minor, his/her parents or other legal representative to the processing of data shall not be considered valid if the processing of the data jeopardises or harms the best interests of the minor.
6. The provisions of this article shall not apply to relations related to the validity of a contract as defined by the Civil Code of Georgia.

Article 8 – Protection of data of a deceased person

1. After a data subject dies, the processing of data concerning him/her shall be permitted:
a) on the grounds specified in Articles 5 and 6 of this Law;
b) unless the processing of such data has been prohibited by the data subject's parent, child, grandchild or spouse (except in cases where the data subject has prohibited in writing the processing of data concerning him/her after his/her death);
c) if 30 years have passed since the death of the data subject;
d) if this is necessary to exercise an inheritance right.
2. The processing of the name, surname, sex, date of birth and date of death of a deceased person shall be permitted irrespective of the circumstances and grounds as provided for by paragraph 1 of this article.

Article 9 – Processing of biometric data

1. Biometric data may be processed only if this is necessary for the purposes of carrying out activities, security, protection of property and prevention of the disclosure of secret information, and these purposes cannot be achieved by other means or involve disproportionate effort, as well as for the purposes of issuing an identity document in accordance with law, identifying a person crossing the state border, combating illegal migration, implementation of international protection, crime prevention, investigation, prosecution, administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences and probation, the re-socialisation and rehabilitation of convicted persons and

former prisoners, the coordination of the process of the referral of minors, the conduct of operative and investigative activities, and ensuring information security and cyber security and in other cases expressly provided for by law.
2. The controller shall be obliged, in accordance with the principles provided for by Article 4 of this Law, to determine in writing, prior to processing, the purpose and amount of biometric data to be processed, the period of storage of these data, the procedure and conditions for their storage and destruction, and the mechanisms for the protection of the rights of the data subject.

Article 10 – Video monitoring

1. Video monitoring is permitted for the purposes of crime prevention, crime detection, public safety, the protection of personal safety and property, the protection of minors (including from harmful influence), the protection of secret information, examination/testing, and for the performance of tasks related to public and/or other legitimate interests, provided that the video monitoring is adequate and proportionate to the purpose of data processing.
2. To carry out video monitoring, the controller shall be obliged, in accordance with the principles provided for by Article 4 of this Law, to determine in writing the purpose and amount of video monitoring, the duration of the video monitoring and the period of storage of the video recording, the procedure and conditions for accessing, storing and destroying the video recording, and the mechanism for the protection of the rights of the data subject, except in cases where a natural person carries out video monitoring in a residential building.
3. Video monitoring of the work process/area of an employee shall only be permitted in exceptional cases where the purposes referred to in paragraph 1 of this article cannot be achieved by other means or involve disproportionate effort.
4. Video monitoring shall not be permitted in changing rooms, hygiene facilities or other places where a data subject has a reasonable expectation of privacy and/or where video monitoring is contrary to generally accepted moral standards.
5. A video monitoring system and video recordings shall be protected from unlawful encroachment and use. The controller shall ensure that any access to the video recordings is recorded, including the time of access and the user name that allow the identification of the person who accessed the video recording.
6. In a residential building, the video monitoring of a common entrance to a residential building and of a common space in a residential building shall be permitted with the written consent of more than half of the owners (if an owner cannot be identified, the consent of a possessor may be obtained), unless the controller/the processor carries out video monitoring to perform his/her statutory duties and the area of video monitoring includes the common entrance and common space of the residential building.
7. The video monitoring of an entrance to an individual property in a residential building shall be permitted only by a decision of the owner/possessor or with his/her written consent, in such a manner that the video monitoring does not harm the legitimate interests of other persons (including those lawfully using the owner's property).
8. The controller/processor shall be obliged to place a warning sign indicating that video monitoring is being carried out in a visible place and, in the case referred to in paragraph 3 of this article, also to warn the employee in writing of the specific purpose(s) of the video monitoring. Where the requirements under this paragraph are met, the data subject shall be deemed to be informed of the processing of data concerning him/her.
9. A warning sign indicating that video monitoring is being carried out shall have an appropriate inscription, a clearly visible image of video monitoring in progress, and the name and contact details of the controller.

Article 11 – Audio monitoring

1. Audio monitoring shall be permitted:
a) with the consent of the data subject;
b) to make a record;
c) to protect important legitimate interests pursued by the controller, provided that appropriate and specific measures are in place to safeguard the rights and interests of the data subject;
d) in other cases expressly provided for by the legislation of Georgia.
2. To carry out audio monitoring, the controller shall be obliged, in accordance with the principles provided for by Article 4 of this Law, to determine in writing and in advance, the purpose and amount of audio monitoring, the duration of the audio monitoring, the procedure and conditions for accessing, storing and destroying the audio recording, and the mechanism for the protection of the rights of the data subject.
3. The controller shall warn the data subject, prior to or upon starting audio monitoring, about the carrying out of audio monitoring, and explain to him/her his/her right to object (if any). The burden of proof of informing the data subject lies with the controller/processor.
4. If the data subject is informed of audio monitoring by means of a warning sign, the warning sign shall have an appropriate inscription, a clearly visible image of audio monitoring in progress, and the name and contact details of the controller.

Article 12 – Processing of data for direct marketing purposes

1. Irrespective of the ground for collecting/obtaining data and their accessibility, data may only be processed for direct marketing purposes with the consent of the data subject.

2. In addition to the name, surname, address, telephone number and e-mail address of the data subject, other data shall be processed for direct marketing purposes with the written consent of the data subject.
3. Prior to obtaining the data subject's consent and when carrying out direct marketing, the controller/processor shall inform the data subject, in clear, simple and understandable language, of his/her right to withdraw his/her consent at any time and of the mechanism/procedure for exercising this right.
4. The controller/processor shall be obliged to terminate the processing of data for direct marketing purposes within a reasonable period after receiving an appropriate request from the data subject, but no later than 7 working days. To ensure that this obligation is met, the controller/processor shall have an obligation to provide information on the withdrawal of consent by the data subject.
5. The controller/processor shall ensure that the data subject has the possibility to request that the processing of data for direct marketing purposes be terminated in the same form in which the direct marketing is carried out, or to determine other available and adequate means to request the termination of the processing.
6. The means referred to in paragraph 5 of this article to request the termination of data processing for direct marketing purposes shall be simple. In addition, the data subject shall be provided with a clear and easily understandable instruction on the use of the means.
7. No fee or other restriction shall be imposed on the data subject for exercising the right to withdraw consent.
8. In the case of direct marketing, the burden of proof for the existence of the data subject's consent, the simplicity of the means of objection, and the ease of understanding, accessibility and adequacy of instructions on the use thereof shall lie with the controller and/or processor.
9. The controller/processor shall record and keep the date and fact of the data subject's consent to the processing of data concerning him/her and the withdrawal of such consent for the duration of the direct marketing and for 1 year after the direct marketing has been discontinued.

Chapter III – Rights of Data Subjects

Article 13 – Right of data subjects to receive information on the processing of data

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not data concerning him/her are being processed and, if requested by the data subject, the following information free of charge:
a) which data concerning him/her are being processed, as well as the grounds for and the purpose of the processing;
b) the source from which the data were collected/obtained;
c) the period for which the data will be stored and, if no specific period can be determined, the criteria used to determine that period;
d) the right of the data subject as provided for by this chapter;
e) the legal basis and purposes of the data transfer, as well as the appropriate data protection safeguards if the data are transferred to another state or an international organisation;
f) the identity of the recipients or the categories of recipients, including information on the ground for and purpose of the transfer, if the data are transferred to a third party;
g) the decision made as a result of automated processing, including profiling, and the logic involved in making such a decision, as well as its impact on the processing and the expected results of the processing.
2. The data subject shall have the right to receive the information referred to in paragraph 1 of this article not later than 10 working days after the request. This period may, in special cases and upon appropriate justification, be extended by no more than 10 working days, of which the data subject shall be notified immediately.
3. The controller shall have the right to provide the data subject with any information necessary to ensure transparent processing in accordance with Article 4(1)(a) of this Law, unless the disclosure of the information is contrary to the law.
4. Unless otherwise provided by the legislation of Georgia, the data subject shall have the right to choose the form of the provision of information as provided for by paragraph 1 of this article. In addition, if the data subject does not request the information in another form, the information shall be provided in the same form in which it was requested.

Article 14 – Right to access and to obtain a copy

1. The data subject shall have the right to access personal data concerning him/her and to obtain copies of such data from the controller free of charge, except in cases where in order to access and/or issue the copies of data:
a) a fee is required under the legislation of Georgia;
b) a reasonable fee is established by the controller because of the resources spent on issuing them in a form other than the data are stored, and/or frequent requests.
2. The data subject shall have the right to access the data referred to in paragraph 1 of this article and/or to obtain copies thereof not later than 10 working days after the request, unless different time limits are set by the legislation of Georgia.
3. The period referred to in paragraph 2 of this article may be extended in special cases and upon appropriate justification by no more than 10 working days, of which the data subject shall be notified immediately.
4. The data subject shall have the right to access the data referred to in paragraph 1 of this article and/or to obtain copies thereof in a form in which they are kept by the controller and/or processor. The data subject shall also have the right to

obtain copies of data concerning him/her in another form in return for a reasonable fee established by the controller and where technically feasible.
5. The fee under paragraph 1(b) of this article shall not exceed the amount of resources actually spent by the controller. The burden of establishing a fee and of proving that its amount is reasonable shall lie with the controller.

Article 15 – Right to the rectification, update and completion of data

1. The data subject shall have the right to request the controller to rectify, update and/or complete erroneous, inaccurate and/or incomplete data concerning him/her.
2. Within not later than 10 working days after the data subject has made the request under paragraph 1 of this article (unless different time limits are set by the legislation of Georgia), the data shall be rectified, updated and/or completed, or the grounds on which the request was refused shall be notified, and the procedure for appealing against the refusal shall be explained, to the data subject.
3. If the controller, independently of the data subject, discovers that the data available to him/her are erroneous, inaccurate and/or incomplete, the controller shall rectify, update and/or complete the data within a reasonable period of time and inform the data subject thereof within 10 working days after the rectification of the data.
4. The controller shall not be obliged to inform the data subject in accordance with paragraph 3 of this article if the rectification, update and/or completion of the data is related to the correction/removal of a technical error.
5. If there are objective circumstances that make it impossible to fulfil the obligation to inform the data subject within the period referred to in paragraph 3 of this article, the controller shall inform the data subject of the change made at the time of the first communication to the data subject.
6. The collector shall inform all the recipients and all respective controllers and processors, to whom the controller transferred the same data, of the update and completion of the data, unless this information cannot be provided due to a large number of controllers/processors or recipients, and/or disproportionately high costs.
7. The persons referred to in paragraph 6 of this article shall rectify, update and/or complete the data within a reasonable period after receiving the respective information.

Article 16 – Right to the termination of the processing, erasure or destruction of data

1. The data subject shall have the right to request the controller to terminate the processing of (including profiling), erase or destroy data concerning him/her.
2. Within not later than 10 working days after the data subject has made the request under paragraph 1 of this article (unless otherwise provided for by the legislation of Georgia), the processing of the data shall be terminated, and/or the data shall be erased or destroyed, or the grounds on which the request was refused shall be notified and the procedure for appealing against the refusal shall be explained to the data subject.
3. The controller shall have the right to refuse the request under paragraph 1 of this article if:
a) one of the grounds provided for in Articles 5 or 6 of this Law exists;
b) data are processed for the purposes of substantiating a legal claim or a statement of defence;
c) the processing of data is necessary for the exercise of the right of freedom of expression or information;
d) data are processed for archiving purposes in the public interest as provided for by law, for scientific or historical research purposes or statistical purposes, and the exercise of the right to the termination of the processing, erasure or destruction of the data would render impossible or substantially impair the achievement of the purposes of the processing.
4. Where any of the grounds provided for by paragraph 3 of this article exists, the controller shall have an obligation to justify the respective ground.
5. The data subject shall have the right to be informed of the termination of the processing, erasure or destruction of the data once the respective action has been taken, without delay and at the latest within 10 working days.
6. The data subject shall have the right, where the data concerning him/her are processed in a publicly available form, to also request the controller to restrict access to the data and/or erase copies of or any internet links to the data.
7. The collector shall inform all the recipients and all respective controllers and processors, to whom the controller transferred the same data, of the termination of the processing, erasure and destruction of the data, unless this information cannot be provided due to a large number of controllers/processors or recipients, and/or disproportionately high costs.
8. The persons referred to in paragraphs 6 and 7 of this article shall, after the receipt of the respective information, terminate the processing of the data and erase or destroy the data.

Article 17 – Right to the blocking of data

1. The data subject shall have the right to request the controller to block data if any of the following circumstances exists:
a) the authenticity or accuracy of the data is contested by the data subject;
b) the processing of the data is unlawful, although the data subject opposes the erasure of the data and requests their blocking;
c) the data are no longer needed for the purposes of the processing, but they are required by the data subject to lodge a complaint/claim;

d) the data subject requests the termination of the processing, erasure or destruction of the data and this request is being considered;
e) there is a need to retain the data for use as evidence.
2. The controller shall be obliged to block the data upon the request of the data subject if one of the circumstances provided for by paragraph 1 of this article applies, unless blocking the data could jeopardise one of the following:
a) the fulfilment by the controller of the duties assigned to him/her by law and/or a law and a subordinate normative act issued on the basis thereof;
b) the performance of tasks falling within the scope of public interest in accordance with law and the exercise by the controller of the powers conferred on him/her under the legislation of Georgia;
c) the legitimate interests of the controller or a third party, unless there is an overriding interest in protecting the rights of a data subject, in particular a minor;
d) the protection of interests as provided for by Article 50(6) of this Law.
3. After the decision to block the data has been made, the controller may decide to unblock the data if any of the grounds provided for by paragraph 2(a)-(d) of this article exists.
4. The data shall be blocked for the period that the reason for blocking them exists, and during this period, if technically feasible, the decision to block the data shall be attached to the relevant data.
5. The data subject shall have the right to be informed of a decision to block the data or of the grounds for refusing to block the data once the decision has been made, without delay and at the latest within 3 working days after the request.
6. Where data are blocked in accordance with paragraph 1 of this article, the data may be processed otherwise than by storage in the following cases:
a) with the consent of the data subject;
b) to substantiate a legal claim or a statement of defence;
c) to protect the interests of the controller or a third party;
d) to protect public interests in accordance with law.

Article 18 – Right to the transmission of data

In the case of the automated processing of data on the grounds provided for by Article 5(1)(a) and (b) and Article 6(1)(a) of this Law, if technically feasible, the data subject shall have the right to receive from the controller data concerning him/her which he/she has provided to the controller in a structured, commonly used and machine-readable format, or to require that the data be transmitted to another controller.

Article 19 – Automated individual decision-making and related rights

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or other similarly significant effects concerning him/her, except where a decision based on profiling is:
a) based on the data subject's explicit consent;
b) necessary for entering into, or performing, a contract between the data subject and a controller;
c) provided for by law or by a subordinate normative act issued within the powers delegated on the basis of the law.
2. Where there is a respective request from the data subject, the controller shall take appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests, including by involving human resources in the decision-making as provided for by paragraph 1(c) of this article, and by giving the right to the data subject to express his/her point of view and to contest the decision.
3. The use of special categories of data in the decision-making as referred to in paragraph 1 of this article shall be permitted only in the cases provided for by Article 6(1)(a), (f) and (j) of this Law, provided that appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 20 – Right to withdraw consent

1. A data subject shall have the right to withdraw his/her consent at any time and without explanation. In such case, the processing of the data shall be terminated, and/or the processed data shall be erased or destroyed, according to the request of the data subject, within not later than 10 working days after the request, provided that no other ground for the processing exists.
2. The data subject shall have the right to withdraw his/her consent in the same form in which it was given.
3. Before withdrawing consent, the data subject shall have the right to request and receive from the controller information on the possible consequences of withdrawing the consent.

Article 21 – Restriction of the rights of data subjects

1. The rights of the data subject under Articles 13-20, 24 and 25 of this Law may be restricted if this is expressly provided for by the legislation of Georgia, does not violate fundamental human rights and freedoms, and is a necessary and proportionate measure in a democratic society, and the exercise of these rights may jeopardise:
a) national security, information security and cyber security and/or defence interests;

b) public safety interests;
c) crime prevention, investigation, prosecution, the administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences and probation, and the conduct of operative and investigative activities;
d) interests relating to financial or economic (including monetary, budgetary and taxation), public health and social protection issues of importance to the country;
e) the detection of the data subject's violations of professional ethical standards, including those of a regulated profession, and the imposition of liability on the data subject;
f) the exercise of the functions and powers of regulatory and/or supervisory bodies in the areas defined by paragraph 1(a), (b), (c), (d), (e), (g) or (i) of this article;
g) the protection of the rights and freedoms, including freedom of expression, of the data subject and others;
h) the protection of state, commercial, professional and other secrets provided for by law;
i) the substantiation of a legal claim or a statement of defence.
2. A measure under paragraph 1 of this article may be applied only to the extent necessary to achieve the purpose of the restriction.
3. If the grounds under paragraph 1 of this article exist, the decision of the controller to restrict, or to refuse the exercise of, the rights of the data subject shall be notified to the data subject, except where the provision of the information would jeopardise the purpose (purposes) of the restriction of the right.
4. The exercise by the data subject of the rights as provided for by Articles 13-20, 24 and 25 of this Law shall be free of charge, subject to the exceptions established by this Law. Where the data subject makes an unreasonable number of requests, the controller may refuse to comply with the request, in which case he/she shall immediately inform the data subject in writing and explain to him/her his/her right to appeal.
5. Where the rights of the data subject are restricted and his/her request is refused, the burden of proof shall lie with the controller.

Article 22 – Right to appeal

1. If the rights as provided for and the rules established by this Law are violated, the data subject shall have the right to apply to the Personal Data Protection Service, to a court and/or a superior administrative body in accordance with procedures established by law.
2. The data subject shall have the right to request the Personal Data Protection Service to make a decision to block the data until a decision is made to complete the consideration of the application.
3. The data subject shall have the right to appeal the decision of the Personal Data Protection Service to a court, in compliance with the conditions and time limits established by the legislation of Georgia.

Chapter IV – Obligations of Controllers and Processors

Article 23 – Obligation to protect the rights of the data subject

1. According to the request of the data subject, the controller shall be obliged to ensure, in accordance with established procedures, the exercise of the rights of the data subject as provided for by Chapter III of this Law, including taking all measures to comply with the requirements of this Law and, if necessary, demonstrate them.
2. The obligations under paragraph 1 of this article shall also apply to the processor in relation to the information kept with/available to him/her.

Article 24 – Informing the data subject where data are collected directly from him/her

1. Where data are collected directly from the data subject, the controller shall be obliged to provide the data subject with at least the following information before or at the beginning of the collection:
a) the identity/name and the contact details of the controller, his/her representative and/or the processor (if any);
b) the purposes and the legal basis of the processing of the data;
c) whether the provision of the data is mandatory, and where the provision of the data is mandatory, the legal consequences of refusal to provide them, as well as the information that the collection/obtaining of the data is required by the legislation of Georgia or is a necessary condition for entering into a contract (if such information exists);
d) the important legitimate interests pursued by the controller or of a third party if the data are processed in accordance with Article 5(1)(i) of this Law;
e) the identity and the contact details of the personal data protection officer (if any);
f) the identity of the recipients or categories of recipients of the data (if any);
g) the planned transfer of data and the existence of appropriate safeguards for the protection of the data, including authorisation to transfer the data (if any) if the controller plans to transfer the data to another state or an international organisation;
h) the period for which the data will be stored and, if no specific period can be determined, the criteria used to determine that period;

i) the right of the data subject as provided for by this chapter.
2. The provision of the information referred to in paragraph 1 of this article shall not be mandatory if it is reasonably foreseeable that the data subject already has such information.
3. The procedure under paragraph 1 of this article shall not apply if special legislation provides for a different procedure for informing the data subject when data are collected from the data subject and that procedure does not result in the infringement of the fundamental rights and freedoms of the data subject. In such case, where there is a written request from the data subject, the controller shall be obliged to provide the data subject with the information referred to in paragraph 1 of this article within 10 working days of the request, unless there are grounds for restricting the right as provided for by Article 21 of this Law.
4. The time limit for providing the information referred to in paragraph 3 of this article may, in special cases and upon appropriate justification, be extended by no more than 10 working days, of which the data subject shall be notified immediately.
5. The controller shall be obliged to provide the information referred to in paragraph 1 of this article to the data subject, especially if the data subject is a minor, in simple and understandable language. This information may be provided orally or in writing (including electronically), unless the data subject requests the provision of the information in writing.

Article 25 – Informing the data subject where data are not collected directly from him/her

1. Where data are not collected directly from the data subject, the collector shall be obliged to provide the data subject with the information referred to in Article 24(1)(a)-(i) of this Law, as well as information as to which data concerning him/her are being processed, and the source of the data, including whether the data have been obtained from a publicly accessible source.
2. The controller shall provide the data subject with the information referred to in paragraph 1 of this article within a reasonable period, or if the data are used to communicate with the data subject, at the time of the first communication with the data subject, or if the disclosure of the data is envisaged, before the data are disclosed, but not later than 10 working day after obtaining the data, unless there are grounds for restricting the right as provided for by Article 21 of this Law.
3. The obligation to provide the information under this article shall not apply to the controller and/or the processor if:
a) the data subject already has the information referred to in paragraph 1 of this article;
b) the collection or disclosure of the data is established by law or required for the performance of statutory duties;
c) the information cannot be provided or involves disproportionate effort, or the fulfilment of the obligation under this article would seriously impair or render impossible the achievement of the legitimate purpose(s) of the processing. In such cases, the controller shall take appropriate measures to protect the rights and legitimate interests of the data subject, including by making general information about the collection of data publicly available/publishing general information about the collection of data in an easily accessible form.

Article 26 – Data masking priority as an initial method used automatically before choosing an alternative approach when creating a new product or service

1. Taking into account the new technologies, development costs, nature, scope, context and purposes of data processing, the expected risks to the rights and freedoms of data subjects, and the principles of data processing, a controller shall take appropriate technical and organisational measures (including pseudonymisation, etc.) when determining the means of data processing and during the data processing. Taking such measures will ensure the effective implementation of data processing principles and the integration of data protection mechanisms in data processing, in order to ensure the protection of the rights of data subjects.
2. When determining the volume and scope of data processing, the periods of data storage and the authority to access such data, a controller shall ensure that technical and organisational measures are taken to process automatically only the volume of such data that is necessary for the specific purpose of the processing. Such measures shall be applied in such a manner that, before choosing an authorised alternative approach, an indefinite number of persons are automatically provided with access to the minimum volume of data.

Article 27 – Data security

1. A controller is obliged to take appropriate technical and organisational measures to ensure the processing of data in accordance with this Law and the confirmation of the compliance of data processing with this Law.
2. A controller and a processor are obliged to take organisational and technical measures that are adequate for the possible and associated risks of data processing (including data pseudonymisation, registration of the access to data, information security mechanisms (confidentiality, integrity, accessibility), etc.), which will ensure the protection of the data against loss or unlawful processing, including destruction, deletion, alteration, disclosure or use.
3. When determining the necessary organisational and technical measures for ensuring data security, a controller and a processor are obliged to take into account the data categories and volume, and the purpose, form and means of data processing and possible threats of violation of the rights of data subjects, and to periodically assess the efficiency of technical and organisational measures taken for ensuring data security, and where necessary, to take adequate measures

and/or update existing measures for ensuring data security.
4. A controller and a processor are obliged to ensure that all operations performed in relation to electronic data (including information on incidents, data collection, data alteration, data access, data disclosure (transfer), data links and data deletion) are registered. When processing non-electronic data, the controller and the processor are obliged to ensure that all operations related to data disclosure and/or alteration (including information on incidents) are registered.
5. Any employee of a data controller and a data processor who is involved in data processing, or who has access to data, is obliged to act within the scope of powers granted to him/her, maintain data secrecy and confidentiality, and to comply with same after the termination of his/her term of office.
6. A controller and a processor are obliged to determine the volume of data to be accessed by employees depending on their scope of authority, and to take adequate measures to safeguard such data from incidents of unlawful data processing by employees, and to identify and prevent such incidents, and to provide information to employees on matters related data security.

Article 28 – Registration of information related to data processing and notifying the Personal Data Protection Service thereof

1. A controller and a special representative (if any) are obliged to ensure, in writing or electronically, the registration of the following data processing information on:
a) the identity / name and contact details of the controller, special representative, personal data protection officer, joint controller, and the processor ;
b) the objectives of the data processing ;
c) the data subjects and the data categories ;
d) the categories of data recipients (including the categories of data recipients from another state or international organisation) ;
e) the transfer of data to another state or international organisation, as well as appropriate guarantees of data protection, including a permit from the Personal Data Protection Service (if any) ;
f) the periods of data storage, and where such periods cannot be specified, the criteria for determining the periods of storage ;
g) a general description of the organisational and technical measures taken for ensuring data security ;
h) information on incidents (if any).
2. A processor and a person involved in data processing in accordance with the procedure established by Article 36(7) of this Law are obliged to ensure, in writing or electronically, the registration of the following data processing information on:
a) the name and contact details of the processor, personal data protection officer, controller, joint controller, and special representative ;
b) the types of data processing carried out for or on behalf of the controller ;
c) the information provided for by paragraph 1(e) of this article, if they participate in the process of transferring data to another state or international organisation ;
d) a general description of the organisational and technical measures taken for ensuring the data security ;
e) information on incidents (if any).
3. A controller, co-controller, processor and a special representative shall provide to the Personal Data Protection Service the information provided for by paragraphs 1 and 2 of this article immediately upon request, but not later than 3 working days after a request.
4. A copy of a court ruling on issuing or refusing to issue a permit to conduct covert investigative actions requested by a law enforcement body, which contains only the particulars and the resolution part, as well as a copy of a court ruling on recognising an investigative action, conducted by a law enforcement body without a court permission , as lawful/ unlawful, which contains only the particulars and the resolution part, shall be submitted to the Personal Data Protection Service in accordance with the procedures determined by the Criminal Procedure Code of Georgia.
5. An electronic communications company shall notify the Personal Data Protection Service about the transfer of electronic communication identification data to a law enforcement body in accordance with the procedure established by Article 136 of the Criminal Procedure Code of Georgia, and the notification shall be sent within 24 hours after such transfer.
6. In the case of urgent necessity, a prosecutor's decree on the conduct of a covert investigative action, which contains only the particulars and the resolution part, shall be submitted as a tangible document to the Personal Data Protection Service by a prosecutor or an investigator, on the instruction of the prosecutor, not later than 12 hours after the time of the start of the covert investigative action as specified in the decree.
7. An electronic copy of a court ruling on the issuance of a permit for conducting a covert investigative action as provided for by Article 143^1(a) of the Criminal Procedure Code of Georgia, which contains only the particulars and the resolution part, as well as an electronic copy of the prosecutor's decree on conducting a covert investigative action, which contains only the particulars and the resolution part, shall be submitted to the Personal Data Protection Service immediately after their receipt by the Agency, via the electronic control system.

Article 29 – Obligation to notify the Personal Data Protection Service about an incident

1. A controller is obliged to register an incident, its resulting outcome, the measures taken, and to notify the Personal Data Protection Service about the incident, not later than 72 hours after the identification of the incident, in writing or electronically, except for the case where it is least expected that the incident would cause significant damage and/or pose a significant threat to fundamental human rights and freedoms.
2. A processor is obliged to notify a controller immediately about an incident.
3. A notification as referred to in paragraph 1 of this article shall contain the following information on:
a) the circumstances, type and time of the incident;
b) the possible categories and volume of data that have been disclosed, damaged, deleted, destroyed, obtained, lost, or altered in a non-authorised manner as a result of the incident, as well as the possible categories and number of data subjects that have been exposed to a threat as a result of the incident;
c) the measures taken or planned by a controller for mitigating or eliminating any possible damage caused by the incident;
d) whether or not, and within what time frame, a controller plans to notify a data subject(s) about the incident in accordance with the procedures established by Article 30 of this Law;
e) the data of a personal data protection officer or other contact persons.
4. If it is impossible to provide the information provided for by paragraph 3 of this article entirely and in full, a controller shall have the right, in agreement with the Personal Data Protection Service, to provide the information gradually, within a reasonable period.
5. If, in accordance with the notification submitted to the Personal Data Protection Service, a controller does not inform or fails to inform a data subject(s) about the incident, the Personal Data Protection Service shall be authorised to make public the available information on the incident considering the circumstances of the incident, the possible damage and/or the number of data subjects, except where one of the circumstances provided for by Article 30(3) of this Law prevails.
6. The procedure provided for by paragraph 5 of this article shall not apply if the notification provided for by paragraph 1 of this article is accompanied by an instruction of a public or private controller that the disclosure of information on the incident would pose a threat to:
a) the interests of state security, information security and cyber security, and/or defence ;
b) the interests of public security ;
c) crime prevention, investigation, a criminal prosecution, the administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences and probation, and operative and investigative activities ;
d) interests related to financial or economic (including monetary, budgetary, and taxation) matters, public health and social protection that are essential for the country.
7. The Personal Data Protection Service is entitled not to disclose information in the cases provided for by paragraph 6 of this article, even if the notification is not accompanied by any of the instructions provided for by paragraph 6 (a-d) of this article.
8. A controller shall notify the Personal Data Protection Service about the circumstances provided for in the relevant sub-paragraph of paragraph 6 of this article in the form of a notification of incident in accordance with the procedure established by paragraph 9 of this article.
9. The criteria for identifying an incident posing a significant threat to fundamental human rights and freedoms as provided for by paragraph 1 of this article, and the procedure for notifying the Personal Data Protection Service about the incident, shall be established by a normative act of the head of the Personal Data Protection Service.
10. A public controller shall specify the appropriate circumstances determined by the relevant sub-paragraph of paragraph 6 of this article in accordance with its own competence/area of activity.
11. The subject of the critical information system, taking into account its category, shall specify the basis of information security and cyber security provided for by paragraph 6(a) of this article, in agreement with the relevant agency competent in the field of information security and cyber security.

Article 30 – Obligation to inform a data subject on the incident

1. If there is a high probability that an incident will cause significant damage and/or pose a significant threat to fundamental human rights and freedoms, a controller is obliged to inform a data subject about the incident immediately, or without unreasonable delay, after the identification of the incident, and to provide, in a simple and understandable language, the following information on:
a) a general description of the incident and the related circumstances;
b) the possible/resulting damage caused by the incident, and the measures taken or planned in order to mitigate or eliminate the damage;
c) the contact details of the personal data protection officer or other persons.
2. If informing a data subject requires disproportionately great efforts, expenses and time, a controller is obliged to make public the information provided for by paragraph 1 of this article or to disseminate it in another form that ensures the possibility of the data subject receiving the information.

3. The obligation provided for by paragraphs 1 and 2 of this article shall not arise where one of the following circumstances exists; namely if:
a) informing a data subject on the incident poses a threat to the interests of the protection of state secrets, the interests of state security, information security and cyber security and/or defence, the interests of public safety, crime prevention, operative and investigative activities, a criminal investigation, a criminal prosecution, the administration of justice, the enforcement of detention and imprisonment, the execution of non-custodial sentences or probation, interests related to financial or economic (including monetary, budgetary, and taxation) matters, public health and social protection that are essential for the country;
b) if a controller has taken appropriate security measures that have resulted in the prevention of a significant risk of violation of fundamental human rights and freedoms.
4. The criteria for identifying an incident posing a significant threat to fundamental human rights and freedoms as provided for by paragraph 1 of this article, the procedures for notifying the Personal Data Protection Service about such incident shall be established by a normative act of the head of the Personal Data Protection Service.

Article 31 – Data protection impact assessment

1. If, taking into account the new technologies, categories and the volume of data, and the purposes and means of data processing, there is a high probability of threat of violation of fundamental human rights and freedoms during data processing, a controller is obliged to carry out a data protection impact assessment in advance.
2. Except for the case provided for by paragraph 1 of this article, the data protection impact assessment shall be mandatory if a controller:
a) makes decisions, in a fully automated manner, including on the basis of profiling, having legal, financial or other significant consequences for a data subject;
b) processes data of a special category of a large number of data subjects;
c) carries out systematic and large-scale monitoring of data subjects' behaviour in places of public gathering.
3. During the data protection impact assessment, a controller is obliged to create a written document containing:
a) a description of the data category, the purposes, proportionality, process and grounds of data processing;
b) an assessment of possible threats of violation of fundamental human rights and freedoms and a description of the organisational and technical measures provided for data security.
4. In the case of a substantial change in the process of data processing, a controller is obliged to update the data protection impact assessment document, to keep the data protection impact assessment document for the entire period of the data processing, and in the case of the termination of data processing, for at least 1 year thereafter.
5. If, as a result of a data protection impact assessment, a high risk of violation of fundamental human rights and freedoms is identified, a controller is obliged to take all necessary measures to mitigate the risk substantially, and where necessary, address the Personal Data Protection Service for consultation. Where the threat of violation of fundamental human rights and freedoms cannot be mitigated by taking additional organisational and technical measures, the data processing shall not be carried out.
6. To address the Personal Data Protection Service on the basis of paragraph 5 of this article a controller shall submit:
a) information on the authority of the controller, joint controller and a processor ;
b) information on the purposes and means of the planned data processing ;
c) information on security measures for protecting the rights and freedoms of a data subject ;
d) the contact details of a personal data protection officer (if any) ;
e) the data protection impact assessment ;
f) other (additional) information in the event of a request by the Personal Data Protection Service.
7. A significant number of data subjects shall be considered to be not less than 3 percent of the population of Georgia, which is calculated in accordance with the results of the latest population census.
8. A data protection impact assessment document as specified in paragraph 3 of this article shall not be subject to disclosure, insofar as it may endanger the interests of state security, information security and cyber security and/or defence, the interests of public security, crime prevention, operative and investigation activities, a criminal investigation, a criminal prosecution, the administration of justice, the enforcement of detention or imprisonment, the execution of non-custodial sentences and probation, interests related to financial or economic (including monetary, budgetary and tax) matters, and public health and social protection, that are of significance for the country, and the prevalent legitimate interests of a controller and a processor.
9. The criteria for determining the circumstances giving rise to the obligation for a data protection impact assessment as provided for by paragraph 1 of this article and the procedure for conducting the assessment shall be established by a normative act of the head of the Personal Data Protection Service.

Article 32 – Obligations of a controller when receiving consent from a data subject and the withdrawing of consent by a data subject

1. If a controller plans to obtain written consent from a data subject with a document that also covers other matters, the controller is obliged to formulate the wording of the consent in the document in a clear, simple and understandable

language and to separate it from other parts of the document.
2. If the consent of a data subject is given within the scope of a contract or service, when determining whether or not the consent was given on a voluntary basis, among other circumstances, it shall be assessed whether the consent is a required term of the contract or service, and whether it is possible to receive the relevant service/enter into the relevant contract without such consent.
3. Before obtaining consent from a data subject, a controller shall ensure that the data subject is informed of his/her right to withdraw the consent.
4. A controller is obliged to immediately terminate the data processing and delete or destroy the processed data if a data subject withdraws his/her consent, unless otherwise provided for by this Law.
5. The obligation determined by paragraph 4 of this article shall not apply to the case provided for by Article 16(3) of this Law.
6. The withdrawal of consent by a data subject shall not lead to the cancellation of legal consequences arising before the withdrawal of the consent and within the scope of the consent.
7. On the basis of a request of a data subject or in the event that this results in legal, financial or other significant consequences for the data subject, a controller is obliged to provide the data subject, prior to the withdrawal of consent by the data subject, with information on the consequences of the withdrawal of consent.
8. A controller is obliged to provide a free, simple and accessible mechanism for withdrawing consent, including the possibility of withdrawing consent in the same form in which the consent was given.
9. In the event of a dispute regarding the existence of a data subject's consent to data processing, a controller shall bear the burden of proving the fact of the existence of the data subject's consent.

Article 33 – Personal data protection officer

1. Public institutions, insurance organisations, commercial banks, micro-finance organisations, credit bureaus, electronic communication companies, airlines, airports, and medical institutions, as well as controllers/processors processing the data of a significant number of data subjects or carrying out systematic and large-scale monitoring of their behaviour, are obliged to appoint or designate a personal data protection officer. The personal data protection officer shall:
a) inform a controller, a processor and their employees on matters related to data protection, including on matters related to the adoption or modification of regulatory legal norms, and provide them with consultation and assistance in terms of the methodology used;
b) participate in the development of internal regulations related to data processing and the data protection impact assessment document, and also monitor whether a controller or a processor complies with the legislation of Georgia and the internal organisational documents;
c) analyse received applications and grievances regarding data processing and make appropriate recommendations;
d) receive consultations from the Personal Data Protection Service, represent a controller and a processor in the relationship with the Personal Data Protection Service, submit information and documents at its request, and coordinate and monitor the execution of its tasks and recommendations;
e) in the event of an application by a data subject, provide him/her with information on data processing and his/her rights;
f) perform other functions for ensuring the improvement of standards of data processing by a controller and a processor.
2. Except for the cases provided for by paragraph 1 of this article, other controllers shall have the right, at their own discretion, to appoint or designate a personal data protection officer.
3. The function of a personal data protection officer may be performed by an employee of a controller or a processor or by other person(s) on the basis of a service contract. The personal data protection officer shall have the right to perform other functions unless they give rise to a conflict of interest.
4. A controller or a processor may appoint or designate a common personal data protection officer provided that he/she completes his/her functions. If the controller or the processor is a public institution, it shall also be permissible to appoint or designate a common personal data protection officer for several state institutions, taking into account the organisational structure and size of the said institutions.
5. A personal data protection officer shall have appropriate knowledge in the field of data protection.
6. A personal data protection officer shall be accountable to the highest governance structure, taking into account the specific circumstances.
7. A controller and a processor shall ensure the proper involvement of a personal data protection officer in the process of taking important decisions regarding data processing, provide him/her with appropriate resources, and ensure his/her autonomy during the carrying out of activities.
8. A controller and a processor are obliged to provide to the Personal Data Protection Service information on the identity and contact details of a personal data protection officer, who is in charge of making such information public; this shall be carried out within 10 working days after the appointment or designation and/or replacement of the relevant personal data protection officer. The controller and the processor are obliged to publish the identity and contact details of the personal data protection officer on a website (if any) in a proactive manner, or through other available means.
9. A controller and a processor, in the case of the temporary absence of a personal data protection officer or the

termination of his/her authority, are obliged, without unjustifiable delay, to grant the authority of the personal data protection officer to another person.
10. The number of controllers and processors with no obligation to appoint or designate a personal data protection officer shall be determined by a normative act of the head of the Personal Data Protection Service. When determining the number of controllers and processors, the head of the Personal Data Protection Service shall take into account the criteria established by paragraph 1 of this article.

Article 34 – Special representative

1. In the case of data processing by a controller/processor who is registered outside Georgia using the technical means available in Georgia, the controller/processor is obliged to appoint or designate a special representative in Georgia before data processing using the technical means available in Georgia. The special representative shall be registered in the manner established by a normative act issued by the Personal Data Protection Service.
2. In the case provided for by paragraph 1 of this article, a controller shall have the right to data processing only after the registration of a special representative.
3. A special representative is obliged to comply with a request and/or decision made by the head of the Personal Data Protection Service in the manner provided for by law.
4. A data subject shall have the right to request, through a special representative, the exercise of his/her rights in relation to a controller/processor registered outside Georgia.
5. The appointment of a special representative shall not relieve a controller/processor registered outside Georgia from the obligation to respond to the request and/or decision made in relation to the relevant controller/processor by the head of the Personal Data Protection Service in the manner provided for by law.
6. The obligation stipulated by paragraph 1 of this article shall not apply to a controller/processor, which is founded in a member state of the European Union, in which case the personal data protection rules applicable in the European Union will apply.
7. The obligation stipulated by paragraph 1 of this article shall not apply to a controller/processor, which is founded in a state with adequate data protection rules recognised by the European Union.

Article 35 – Joint controllers

1. Where joint controllers are involved in data processing, they are obliged to determine, in advance, each joint controller's written obligations and responsibilities related to compliance with the requirements of this Law, including in relation to the protection of the rights of data subjects and the obligations stipulated by Articles 13 through 20, and Articles 24 and 25 of this Law.
2. If joint data processing is provided for by the legislation of Georgia, the obligations and responsibilities of each joint controller shall be determined by a relevant legal act and/or written agreement.
3. Information on the distribution of obligations and responsibilities between joint controllers shall be available to data subjects. Their rights to apply to joint controllers individually shall not be restricted.

Article 36 – Processor

1. A processor may carry out data processing only on the basis of a legal act or a written agreement concluded with a controller, which shall specify the grounds and purposes of the data processing, the categories of data to be processed, the term of data processing, and the rights and obligations of a controller and a processor.
2. The written agreement provided for by paragraph 1 of this article shall also include the following obligations of a processor:
a) to carry out data processing only in accordance with the written instructions or guidelines of a controller;
b) to ensure that a natural person who directly participates in data processing has an obligation to maintain confidentiality;
c) to ensure data security in accordance with this Law;
d) to delete or transfer data to a controller in the case of the cancellation or termination of the agreement provided for by paragraph 1 of this article, and to delete their copies, unless an obligation to keep them is established by the legislation of Georgia;
e) to provide appropriate information to a controller in order to ensure compliance with the obligations established by this Law and the monitoring of data processing by the controller.
3. A legal act as provided for by paragraph 1 of this article or a written agreement concluded with a controller in order to ensure data security and the protection of the data subject's rights may provide for the obligation of a processor to provide assistance to the controller.
4. A processor shall not be allowed to carry out further data processing for purposes other than those determined by an agreement or a legal act.
5. A processor shall be allowed to carry out data processing only if the processor ensures the taking of appropriate organisational and technical measures to protect the rights of data subjects and if he/she ensures compliance with the requirements of law. An agreement on data processing may not be concluded if, due to the activities and/or purposes of

the processor, there is a high risk of inappropriate data processing, or the risk of violation of the rights of data subjects.
6. A controller is obliged to request from a processor, in advance, information on statutory data processing, and to monitor data processing by the processor.
7. Unless otherwise provided for by the legislation of Georgia, a processor may not transfer his/her rights and duties, fully or partially, to another person without the prior written consent of a controller. The consent of the controller shall not relieve the processor from the relevant obligations and responsibilities.
8. Unless otherwise provided for by the legislation of Georgia, in the event of a dispute between a processor and a controller in relation to data processing, the processor is obliged to immediately terminate data processing and transfer all the data in his/her possession to the controller.
9. In the event of the cancellation or invalidity of a legal act (or a relevant provision therein), or the termination of a written agreement as provided for by paragraph 1 of this article, data processing shall be terminated and the processed data shall be immediately transferred to a controller in full.
10. A processor is obliged to take appropriate organisational and technical measures to assist a controller in the fulfilment of his/her obligations related to the exercise of the rights of a data subject.

Chapter V – International Data Transfer

Article 37 – Transfer of data to another state and international organisation

1. The transfer of data to another state and international organisation shall be allowed if the requirements for data processing provided for by this Law and appropriate safeguards in the relevant state or international organisation are in place for ensuring data protection and the protection of data subjects' rights.
2. In addition to paragraph 1 of this article, the transfer of data to another state and international organisation shall be allowed if:
a) the transfer of data is envisaged by an international treaty and the agreements of Georgia;
b) a controller provides appropriate safeguards for data protection on the basis of an agreement concluded between the controller and the relevant state, the appropriate public institution of such state, a legal person or a natural person, or an international organisation;
c) the transfer of data is stipulated by the Criminal Procedure Code of Georgia (for the purpose of carrying out investigative action), the Law of Georgia On the Legal Status of Aliens and Stateless Persons, the Law of Georgia On International Cooperation in Criminal Matters, the Law of Georgia On International Cooperation in Law Enforcement, and a normative act adopted on the basis of the Organic Law of Georgia On the National Bank of Georgia or the Law of Georgia On Facilitating the Prevention of Money Laundering and the Financing of Terrorism;
d) a data subject gives written consent after receiving information on the lack of proper safeguards for data protection in the relevant state and on possible threats;
e) the transfer of data is necessary to protect the vital interests of a data subject and the data subject is physically or legally incapable to give consent to such data processing;
f) there is a lawful public interest (including for the purposes of crime prevention, investigation, identification and criminal prosecution, the execution of a sentence and carrying out operative and investigation actions) and the transfer of data is a necessary and proportionate measure in a democratic society.
3. On the basis of paragraph 2(b) of this article, data transfer shall be allowed only after obtaining a permit from the Personal Data Protection Service, and the procedure for issuing such permit shall be established by a normative act of the head of the Personal Data Protection Service.
4. In the case of data transfer on any of the grounds stipulated in paragraph 2 of this article, a controller/processor is obliged to take necessary organisational and technical measures to safeguard such data transfer.
5. In the case of data transfer on the basis of paragraph 2(b) of this article, an agreement on data transfer shall provide that the provisions therein are legally binding.
6. Data transferred to another state or international organisation may be further transferred to a third party only if such data transfer serves the initial purpose of data transfer and meets the basis for data transfer and guarantees adequate safeguards for data protection as provided for by this article.

Article 38 – Establishing adequate safeguards for data protection

1. The existence of adequate safeguards for data protection in another state and/or international organisation shall be assessed by the Personal Data Protection Service on the basis of international obligations and regulatory legislation relating to data protection, guarantees for the protection of the rights and freedoms of data subjects (including effective legal protection mechanisms), rules for further international data transfer, and the analysis of the existence, powers and activities of an independent data protection supervisory body.
2. A list of states and international organisations in which adequate data protection guarantees are ensured shall be determined by a normative act of the head of the Personal Data Protection Service.
3. The list determined by a normative act of the Personal Data Protection Service shall be reviewed at least once every 3 years. If a state and/or international organisation no longer meets the conditions provided for by paragraph 1 of this

article, appropriate changes shall be made in the list as provided for by a normative act, which shall not have retroactive force.

Chapter VI –Principles of Activities of the Personal Data Protection Service and Guarantees for the Exercise of its Powers, the Powers of the Head of the Personal Data Protection Service, his/her Election, Inviolability, Incompatibility of Duties and Early Termination of his/her Powers

Article 39 – Status and principles of activities of the Personal Data Protection Service

1. The Personal Data Protection Service is an independent state body established and operating on the basis of law.
2. The Personal Data Protection Service shall be guided by the Constitution of Georgia, the international treaties of Georgia, generally recognised principles and norms of international law, this Law and other relevant legal acts.
3. The principles of activities the Personal Data Protection Service are:
a) legality;
b) the protection of human rights and freedoms;
c) independence and political neutrality;
d) objectivity and impartiality;
e) professionalism;
f) the ensuring of secrecy and confidentiality.
4. The procedure for submitting a report to the Parliament of Georgia by the Personal Data Protection Service shall be determined by this Law and the Rules of Procedure of the Parliament of Georgia.

Article 40 – Powers of the head of the Personal Data Protection Service

1. The head of Personal Data Protection Service shall:
a) direct the Personal Data Protection Service and take decisions on matters related to the activities of the Service;
b) determine the structure of the Personal Data Protection Service, and the powers of its structural units and employees, and establish procedures for employees serving at the Personal Data Protection Service;
c) approve a staff list of employees of the Personal Data Protection Service, and remuneration procedures and the amount of remuneration, in accordance with the legislation of Georgia;
d) determine the functions and duties of the first deputy and deputy head of the Personal Data Protection Service and delegate powers;
e) appoint and dismiss employees of the Personal Data Protection Service;
f) assign a special state rank (the special rank) to an employee of the Personal Data Protection Service (except for a person employed under an employment contract) and demote from the special state rank in accordance with the procedure established by the legislation of Georgia;
g) represent the Personal Data Protection Service in relations with state bodies, and international and other organisations;
h) ensure the protection and targeted use of state property transferred to the Personal Data Protection Service;
i) exercise other powers in accordance with law.
2. The head of the Personal Data Protection Service shall, within the scope of his/her powers, issue subordinate normative acts called orders on matters related to the activities of the Personal Data Protection Service.
3. The head of the Personal Data Protection Service shall issue individual legal acts, including decisions, orders, and instructions, on the basis of an appropriate normative act and within the scope of his/her powers.

Article 41 – Election of the head of the Personal Data Protection Service and his/her term of office

1. A citizen of Georgia with no criminal record who has higher education in law and at least 5 years of work experience in the system of justice and law enforcement bodies or in the field of human rights, as well as with a high professional and moral reputation, may be elected to the position of head of the Personal Data Protection Service.
2. A competition for the selection of the head of the Personal Data Protection Service shall be announced and a competition commission shall be established by an order of the Prime Minister of Georgia. The members of the competition commission shall be:
a) a representative of the Government of Georgia ;
b) the chairperson of the Human Rights and Civil Integration Committee of the Parliament of Georgia ;
c) the chairperson of the Legal Issues Committee of the Parliament of Georgia ;
d) the deputy chairperson of the Supreme Court of Georgia ;
e) the first deputy or the deputy General Prosecutor of Georgia ;
f) the Public Defender of Georgia or a representative of the Public Defender of Georgia ;
g) a person with appropriate experience, including experience of working in the field of the protection of human rights and/or data protection, who has been selected by the Public Defender of Georgia through an open competition or without a competition from among members of non-entrepreneurial (non-commercial) legal entities.
3. Not earlier than 14 weeks and not later than 12 weeks before the termination of the term of office of the head of the Personal Data Protection Service, and in the case of early termination of the term of office, within 2 weeks after the

termination of the term of office, the agencies and institutions determined by paragraph 2 of this article shall inform the Prime Minister of Georgia of the identity of the members of a competition commission for the selection of the head of the Personal Data Protection Service. 7 days after the expiry of the deadline for the nomination of the members of the competition commission, the Prime Minister of Georgia shall convene the first meeting of the competition commission. The meeting of the competition commission shall be quorate if the majority of the full composition of the competition commission is present. The competition commission shall elect the chairperson of the competition commission from among its members at the first meeting by a majority of votes and shall approve the regulations of the competition commission for the selection of the head of the Personal Data Protection Service within 1 week, which shall include the rules of the activities of the competition commission, as well as the deadline and procedures for the nomination of candidacies for the head of the Personal Data Protection Service.
4. The competition commission for the selection of the head of the Personal Data Protection Service shall select not less than 2 and not more than 5 candidates for the head of the Personal Data Protection Service by a majority of votes of all members present, and shall nominate them to the Prime Minister of Georgia. Taking into account the number of selected candidates, the number of candidates of different genders shall be maximally equal.
5. The Prime Minister of Georgia shall, within 10 days, nominate 2 candidates to the Parliament of Georgia for the selection to the position of the head of the Personal Data Protection Service.
6. The Parliament of Georgia shall elect the head of the Personal Data Protection Service in accordance with the rules established by the Rules of Procedure of the Parliament of Georgia not later than 14 days after the nomination of candidates. If the term fully or partially coincides with the period between the sessions of the Parliament of Georgia, the time period specified by this paragraph for the election of the head of the Personal Data Protection Service shall be equally extended. If the Parliament of Georgia fails to elect the head of the Personal Data Protection Service through the voting or if both candidates refuse to be elected to the position of the head of the Personal Data Protection Service before the voting, the Prime Minister of Georgia shall announce a repeated competition within 2 weeks.
7. If the head of the Personal Data Protection Service was elected before the expiry of the term of office of the current head of the Personal Data Protection Service, the powers of the newly elected head of the Personal Data Protection Service shall take effect on the day following the expiry of the term of office of the current head of the Personal Data Protection Service. If the head of the Personal Data Protection Service was elected after the expiry of the term of office of the head of the Personal Data Protection Service or before the termination of his/her term of office, the powers of the newly elected head of the Personal Data Protection Service shall take effect on the day following his/her election.
8. The term of office of the head of the Personal Data Protection Service shall be 6 years. A person may not be elected to the position of head of the Personal Data Protection Service twice in succession. The head of the Personal Data Protection Service may not perform his/her duties after the expiry or the termination of the term of office.
Law of Georgia No 4210 of 29 May 2024 – website, 12.6.2024

Article 42 – First deputy and deputy head of the Personal Data Protection Service

1. The head of the Personal Data Protection Service shall have a first deputy and a deputy, whom he/she shall appoint to the positions by an order. Upon the expiry or termination of the term of office of the head of the Personal Data Protection Service, the term of office of the first deputy and deputy head of the Personal Data Protection Service shall cease as soon as the newly elected head of the Personal Data Protection Service starts the exercise of powers in accordance with the procedure established by this Law.
2. In the case of the absence of the head of the Personal Data Protection Service, his/her failure to exercise powers, the suspension, expiry or termination of his/her powers, the powers of the head of the Personal Data Protection Service shall be exercised by the first deputy head of the Personal Data Protection Service, and in the absence of the first deputy, by the deputy head of the Personal Data Protection Service. During the performance of the duties of the head of the Personal Data Protection Service, the first deputy and the deputy head of the Personal Data Protection Service shall enjoy the powers and legal guarantees granted to the head of the Personal Data Protection Service.

Article 43 – Inviolability of the head of the Personal Data Protection Service

1. The head of the Personal Data Protection Service shall be inviolable. The criminal prosecution, detention or arrest of the head of the Personal Data Protection Service, the search of his/her residence, workplace or car, or a personal search, can only be carried out with the prior consent of the Parliament of Georgia. An exception is the case when he/she has been caught in flagrante delicto, which shall be immediately reported to the Parliament of Georgia. If the Parliament of Georgia does not give its consent within 48 hours, the arrested or detained head of the Personal Data Protection Service shall be released immediately.
2. In the event that the Parliament of Georgia gives its consent to the arrest or detention of the head of the Personal Data Protection Service, his/her powers shall be suspended by a resolution of the Parliament of Georgia before the resolution/judgment on the termination of a criminal prosecution is issued or a court judgment enters into legal force.
3. The personal security of the head of the Personal Data Protection Service shall be duly ensured by the relevant state bodies.

Article 44 – Incompatibility of the duties of the head of the Personal Data Protection Service

1. The position of the head of the Personal Data Protection Service shall be incompatible with membership of the representative bodies of state authorities and municipalities, any position in public and state services, and with other paid activities, except for scientific, pedagogical and artistic activities. The head of the Personal Data Protection Service may not engage in entrepreneurial activities, or directly exercise the powers of a permanent head of a business entity, or a member of a supervisory, control, audit or advisory body, or be a member of a political party or participate in political activities.
2. The head of the Personal Data Protection Service shall not be allowed to participate in gatherings and demonstrations supporting or opposing the political union of citizens.
3. The person elected to the position of the head of the Personal Data Protection Service is obliged to terminate any activities which are incompatible with the position or to resign from a position which is incompatible with his/her status within 10 days after the election. Until the person elected to the position of the head of the Personal Data Protection Service terminates activities which are incompatible with the position or resigns from a position which is incompatible with his/her status, he/she shall not be authorised to start exercising the powers of the head of the Personal Data Protection Service. If the head of the Personal Data Protection Service does not comply with the requirements established by this paragraph within the said period, his/her powers shall be terminated.

Article 45 – Termination of the powers of the head of the Personal Data Protection Service

1. The powers of the head of the Personal Data Protection Service shall be terminated if:
a) he/she has lost the citizenship of Georgia;
b) he/she has not been able to exercise his/her powers for 4 consecutive months due to his/her health condition;
c) a court's judgement of conviction has entered into legal force;
d) he/she has been recognised by a court as a recipient of support (unless otherwise determined by the court's judgment), as missing or has been declared dead;
e) he/she has occupied a position incompatible with his/her status or carries out activities incompatible with the position;
f) he /she has resigned voluntarily;
g) he/she has died.
2. In the case provided for by paragraph 1 of this article, the powers of the head of the Personal Data Protection Service shall be considered terminated from the moment of the occurrence of the relevant circumstances, of which the Chairperson of the Parliament of Georgia shall immediately inform the Parliament of Georgia. The Parliament of Georgia shall terminate the powers of the head of the Personal Data Protection Service after receiving the information from the Chairperson of the Parliament of Georgia.

Article 46 – Organisational and financial support of the Personal Data Protection Service

1. The structure, the rules for activities and the distribution of powers among employees of the Personal Data Protection Service shall be established by the regulations of the Personal Data Protection Service, which shall be approved by the head of the Personal Data Protection Service.
2. An employee of the Personal Data Protection Service (except for the head, first deputy head and the head of the Personal Data Protection Service) shall be a public servant. The Law of Georgia on Public Service shall apply to employees of the Personal Data Protection Service under the procedures established by the same law, unless otherwise provided for by this Law or a normative act of the head of the Personal Data Protection Service issued on the basis of this Law.
3. The activities of the Personal Data Protection Service shall be financed from the State Budget of Georgia. The allocations necessary for the activities of the Personal Data Protection Service shall be determined under a separate code of the State Budget of Georgia. The current expenses allocated from the State Budget of Georgia for the Personal Data Protection Service, as compared to the amount budgeted for the previous year, may be reduced only with the prior approval of the head of the Personal Data Protection Service.

Article 47 – Independence of the Personal Data Protection Service

1. The Personal Data Protection Service shall be independent in exercising its powers and shall not be subject to any body or official. Any influence on the head of the Personal Data Protection Service or the employees of the Personal Data Protection Service, and any unlawful interference in their activities, shall not be allowed and shall be punishable by law.
2. In order to ensure the independence of the Personal Data Protection Service, the State is obliged to create appropriate conditions for its activities.
3. The head of the Personal Data Protection Service shall have the right not to testify in connection with the carrying out of the functions of controlling the lawfulness of data processing, conducting covert investigative actions and activities carried out in the electronic data identification central bank due to a fact that has been disclosed to him/her during his/her term of office as the head of the Personal Data Protection Service. Such right shall be preserved by him/her after the termination of his/her powers as the head of the Personal Data Protection Service.

Article 48 – Annual report of the Personal Data Protection Service

1. Once a year, not later than 31 March, the head of the Personal Data Protection Service shall submit to the Parliament of Georgia a report on the status of data protection in Georgia, the monitoring of the conduct of covert investigative actions, and the activities carried out in the electronic data identification central bank.
2. The annual report of the Personal Data Protection Service shall contain information on the activities carried out by the Personal Data Protection Service in the field of data protection during the reporting period, general assessments related to the status of data protection in Georgia, conclusions and recommendations, information on significant violations identified during the year and measures taken, and general statistical information on the activities carried out in the field of monitoring the conduct of covert investigative actions.
3. Once a year, the head of the Personal Data Protection Service shall submit a report on the results of monitoring the investigative actions provided for by Articles 136 - 138 of the Criminal Procedure Code of Georgia, and the covert investigative actions provided for by Article 143^1(1)(a-b) of the same Code, to the Parliamentary Committee and the Trust Group determined in accordance with the procedures established by the Parliamentary Bureau on the basis of the Rules of Procedure of the Parliament of Georgia.
4. Information on the activities carried out by the Personal Data Protection Service, taking into account the limitations established by this article, shall be made public through the website of the Personal Data Protection Service.
5. The Personal Data Protection Service shall be authorised to publish a special report at any time on its own initiative on issues related to its activities and which it considers important.

Law of Georgia No 4210 of 29 May 2024 – website, 12.6.2024

Chapter VII – Powers of the Personal Data Protection Service in the Fields of Data Protection and Monitoring the Conduct of Covert Investigative Actions

Article 49 – Main fields of activities of the Personal Data Protection Service in the field of data protection

The Personal Data Protection Service shall monitor the lawfulness of data processing in Georgia. The main fields of activities of the Personal Data Protection Service in the field of data protection shall be to:
a) provide consultations on matters related to data protection;
b) review applications related to data protection;
c) examine (inspect) the lawfulness of data processing;
d) inform the public on the data protection status in Georgia, and important events related thereto, and ensure the raising of awareness among the public.

Article 50 – Review of applications of data subjects by the Personal Data Protection Service

1. The Personal Data Protection Service is obliged to review the applications of data subjects regarding data processing and to take the measures provided for by the legislation of Georgia.
2. Within 10 days after receiving a data subject's application, the Personal Data Protection Service shall take a decision on the measures to be taken, and inform the applicant thereof.
3. The Personal Data Protection Service shall be authorised to carry out an inspection in order to study and investigate the circumstances related to a data subject's application. Any processor and/or controller is obliged to transfer the relevant material, information and/or documents to the Personal Data Protection Service upon request.
4. The period for reviewing an application of a data subject by the Personal Data Protection Service shall not exceed 2 months. On the basis of a grounded decision of the Personal Data Protection Service, the period of review of an application of a data subject may be extended for not more than 1 month.
5. The Personal Data Protection Service shall be authorised to suspend the review of a data subject's application on the grounds of a request for additional material, information and/or documentation, of which the data subject shall be informed. The review of the data subject's application shall continue where such grounds no longer exist. The period of suspension shall not be included in the period provided for by paragraph 4 of this article.
6. The Personal Data Protection Service shall be authorised to take a decision on data blocking before the review of the data subject's application is completed. Despite the blocking of data, the data processing may continue if it is necessary to protect the vital interests of a data subject or a third party, or for the purposes of the security and defence of the State.
7. After reviewing the application of a data subject, the Personal Data Protection Service shall take a decision on one of the measures provided for by Article 52 of this Law, and inform the data subject and a processor and/or a controller thereof in accordance with the procedure and within the time frame specified by the legislation of Georgia.

Article 51 – Inspection by the Personal Data Protection Service

1. The Personal Data Protection Service shall be authorised to carry out, on its own initiative or based on an application of an interested person, an inspection of any controller and/or processor. A decision to carry out an inspection provided for by this article shall be taken by the Head of the Personal Data Protection Service.
2. Inspection by the Personal Data Protection Service involves:
a) determining compliance with the principles of data processing and the existence of legal grounds for data processing;

b) checking the compliance of organisational and technical measures and procedures implemented for data security with the requirements of the legislation of Georgia;
c) the checking of the lawfulness of data transfer to another state and international organisation;
d) checking compliance with the rules and requirements of this Law and other normative acts with respect to data protection.
3. During an inspection, the Personal Data Protection Service shall be authorised to request from any institution, natural and/or legal person, documents and/or information, including information containing state, tax, banking, commercial, professional secrets and/or data, as well as materials and/or documents and/or information describing operative and investigative activities and criminal investigations, which constitute state secrets and are necessary to carry out the inspection within the scope determined by paragraph 2 of this article.
4. A controller and/or a processor is obliged to provide any material, information and/or document to the Personal Data Protection Service immediately, within not later than 10 working days, if a response to the request for information requires:
a) finding and processing information in another institution or structural unit, or consulting with the said institution or unit;
b) searching for and processing a significant volume of information/documents.
5. The Personal Data Protection Service shall be authorised to extend the period referred to in paragraph 4 of this article by not more than 10 working days based on a substantiated application of a controller and/or a processor.
6. The Personal Data Protection Service shall be authorised to visit any institution and organisation for inspection and to obtain any document and information, including information containing state, tax, banking, commercial, professional secrets and/or data, as well as materials and/or documents and/or information describing operative and investigative activities and criminal investigations, which constitute state secrets, irrespective of their content and mode of storage.
7. Taking into account the results of an inspection, the Personal Data Protection Service shall be authorised to apply the measures provided for in Article 52 of this Law.
8. An employee of the Personal Data Protection Service is obliged to secure information containing any kind of secret and not to disclose the secret information that he/she has become aware of in the course of performing his/her official duties. Such obligation shall survive after the termination of the powers of an employee of the Personal Data Protection Service.

Article 52 – Application of measures by the Personal Data Protection Service

1. If the Personal Data Protection Service identifies a violation of this Law or another normative act regulating data processing, it shall be authorised to apply one, or simultaneously more than one, of the following measures:
a) require the remedy of any violations and shortcomings related to data processing in the manner and within the period specified by it;
b) require the suspension or termination of data processing, if the measures and procedures implemented by a controller or a processor for ensuring data security do not comply with the requirements of the legislation of Georgia;
c) require the termination of data processing, the blocking, erasure, destruction or depersonalisation of data, if it believes that the data are being processed in violation of the legislation of Georgia;
d) require the termination of data transfer to another state and international organisation, if the data transfer is being carried out in violation of the legislation of Georgia;
e) provide written advice and recommendations to a controller and/or a processor in the case of a minor violation of the procedures related to data processing;
f) impose administrative liability on an offender.
2. A controller and/or a processor is obliged to fulfil the requirements of the Personal Data Protection Service within the period determined by the latter, and to inform the Personal Data Protection Service thereof.
3. If a controller and/or a processor fails to comply with the requirements of the Personal Data Protection Service, the Personal Data Protection Service shall have the right to apply to a court, a law enforcement body and/or a state institution supervising (regulating) the respective area, as provided for by the legislation of Georgia.
4. If the Personal Data Protection Service identifies an administrative offence, it shall be authorised to draw up an administrative offence report and, accordingly, to impose administrative liability on a controller and/or a processor in accordance with this Law and the Administrative Offences Code of Georgia.
5. If, in the course of performing its activities, the Personal Data Protection Service believes that there are elements of a crime, it shall inform the authorised state body thereof as provided for by law.
6. Compliance with the decisions of the Personal Data Protection Service in the area of data protection shall be mandatory and may only be appealed in a court according to the procedure established by law.

Article 53 – Consultation and implementation of educational activities by the Personal Data Protection Service

1. If requested, the Personal Data Protection Service is obliged to provide consultations to state authorities, municipal bodies, other public institutions, legal entities under private law, and natural persons on any issue related to data processing and data protection.
2. The Personal Data Protection Service shall carry out educational activities on issues related to data processing and data

protection.

Article 54 – Monitoring covert investigative actions and activities carried out in the central bank of electronic communication identification data

1. During the conduct of a covert investigative action, namely the secret eavesdropping and recording of telephone communication, as determined by Article 143^1(1)(a) of the Criminal Procedure Code of Georgia, the Personal Data Protection Service shall monitor:
a) the lawfulness of data processing, through the electronic control system;
b) the lawfulness of data processing, through the special electronic control system;
c) the lawfulness of processing of data by a controller/processor (inspection).
2. The Personal Data Protection Service shall carry out the monitoring of the investigative activities provided for by Articles 136-138 of the Criminal Procedure Code of Georgia by comparing the information provided by courts, the Prosecutor's Office, and the providers of electronic communication services, and by checking (inspecting) the lawfulness of the processing of data by a controller/processor.
3. The Personal Data Protection Service shall carry out the monitoring of the covert investigative actions provided for by Article 143^1(1)(b), (d) and (f) of the Criminal Procedure Code of Georgia by checking (inspecting) the lawfulness of the processing of data by a controller/processor.
4. The Personal Data Protection Service shall carry out the monitoring of the covert investigative actions provided for by Article 143^1(1)(e) of the Criminal Procedure Code of Georgia by checking (inspecting) the lawfulness of the processing of data by a controller/processor, as provided for by this Law. If the checking (inspection) is carried out in the case provided for by this paragraph, information about the identity of a person participating in the conduct of the covert investigative actions (except for a data subject, an investigator and a prosecutor) and his/her participation in the process of checking (inspection), as well as information on the characteristics of the operational and operational-technical equipment used during the conduct of the covert investigative actions provided for by this paragraph, may be requested only upon the approval of the head of the body conducting the covert investigative actions. The carrying out of the checking (inspection) in the case provided for by this paragraph shall not imply direct participation in the process of preparing/conducting the covert investigative action and the on-site inspection of a disguised residential or service premises or other disguised facilities and buildings.
5. The Personal Data Protection Service shall monitor the conduct of the covert investigative actions provided for by Article 143^1(1)(c) of the Criminal Procedure Code of Georgia, as well as the application of the measure provided for by Article 7(3)(b) of the Law of Georgia on Operative and Investigative Activities, with a special electronic control system for real-time location and by checking (inspecting) the lawfulness of processing data by a controller/processor.
6. The Personal Data Protection Service shall monitor the activities carried out in the central bank of electronic communication identification data through the electronic control system of the central bank of electronic communication identification data and by checking (inspecting) the lawfulness of processing data by a controller/processor.
7. During the checking (inspection) of the Agency, the Personal Data Protection Service shall be authorised to:
a) enter the area of limited access of the Agency and monitor the implementation of activities by the authorised bodies in an on-going mode;
b) acquire the legal documents and technical instructions regulating the activities of the Agency (including those containing state secrets);
c) obtain information on the technical infrastructure used for the purposes of covert investigative actions and inspect the infrastructure;
d) request explanations from Agency employees with respect to individual issues identified during the checking (inspection);
e) exercise other powers provided for by this Law.
8. Employees of the Agency are obliged to cooperate with the Personal Data Protection Service, to provide the Personal Data Protection Service with requested information and documents in full, and to provide explanations regarding the individual issues identified during the checking (inspection).

Chapter VIII – Legal Protection and Social Security of Employees of the Personal Data Protection Service, and Employees of the Structural Unit Carrying out Official Inspections of the Personal Data Protection Service

Article 55 – Legal protection of employees of the Personal Data Protection Service

1. In the course of performing his/her official duties, an employee of the Personal Data Protection Service is a representative of the state authority and is protected by the State. The fulfilment of a lawful request of an employee of the Personal Data Protection Service is mandatory for everyone.
2. No one has the right to interfere with the official activities of an employee of the Personal Data Protection Service, except for the cases provided for by law.
3. Obstructing an employee of the Personal Data Protection Service in the performance of his/her duties, encroaching

upon his/her honour and dignity, resisting, threatening, or using violence against him/her, or encroaching upon his/her life, health or property, shall result in the imposition of liability as provided for by the legislation of Georgia. In the case of obtaining information on the encroachment upon the life, health and property of the Head of the Personal Data Protection Service, the First Deputy or Deputy Head of the Personal Data Protection Service, an employee of the Personal Data Protection Service or his/her family members, in connection with the exercise of official powers, the state authorities are obliged to apply the measures provided for by law for their personal safety and the safety of their property.
4. An employee of the Personal Data Protection Service shall refuse to comply with an obviously unlawful order or instruction, if he/she had known or should have known about its unlawfulness, and shall act within the scope of law.
5. An employee of the Personal Data Protection Service shall inform the Head of the Personal Data Protection Service in the case of receiving an obviously unlawful order or instruction.
6. An employee of the Personal Data Protection Service who refuses to comply with an obviously unlawful order or instruction shall not be held liable.
7. A person giving an obviously unlawful order or instruction to an employee of the Personal Data Protection Service shall be held liable according to the procedure established by law.
8. An employee of the Personal Data Protection Service shall have the right to apply to a court to protect his/her rights and freedoms.
9. An employee of the Personal Data Protection Service shall be given an identity card and/or a special badge to confirm his/her official powers, the form and the procedure of issuance of which shall be determined by the Head of the Personal Data Protection Service.

Article 56 – Social security of the employees of the Personal Data Protection Service

1. The State shall ensure the social security of the employees of the Personal Data Protection Service.
2. Unless otherwise provided for by the legislation of Georgia, the social security guarantees of an official provided for by the Law of Georgia on Public Service shall apply to the employees of the Personal Data Protection Service (including the social security guarantees related to bodily injury or death while performing official duties).
3. An employee of the Personal Data Protection Service shall have:
a) an official salary determined in accordance with paragraph 5 of this article;
b) a salary increment and monetary reward as determined by paragraph 5 of this article and the Law of Georgia on Remuneration in Public Institutions;
c) if an employee has a special rank, the rank salary corresponding to such rank;
d) a salary increment according to the years of service;
e) other increments and compensations provided for by the legislation of Georgia.
4. A respective employee of the Personal Data Protection Service shall have the right to receive state compensation or a state pension as provided for by the legislation of Georgia.
5. The amount of and the procedure for the remuneration of an employee of the Personal Data Protection Service, the amounts of the rank salary and increments according to the years of service, as well as the amounts of other increments and compensations provided for by the legislation of Georgia, shall be determined by the normative acts of the Head of the Personal Data Protection Service, and other legislative and subordinate normative acts of Georgia.
6. An employee of the Personal Data Protection Service shall be subject to mandatory state insurance. The matters related to the state insurance of family members of the employees of the Personal Data Protection Service (including the category of family members) shall be determined by the Head of the Personal Data Protection Service.
7. The special ranks of the employees of the Personal Data Protection Service shall be determined by the Law of Georgia on Special State Ranks.

Article 57 – Selection, appointment, and powers of employees of the structural unit carrying out an official inspection of the Personal Data Protection Service

1. An employee of the structural unit carrying out an official inspection of the Personal Data Protection Service (except for the case provided for by paragraph 2 of this article) shall be appointed on the basis of a competition, by an order of the Head of the Personal Data Protection Service. The rules and conditions of the competition for the selection and appointment of an employee of the structural unit carrying out an official inspection of the Personal Data Protection Service, as well as the qualification requirements of a person to be appointed (the basic requirements, which should not be less than the basic requirements established by Article 27 of the Law of Georgia on Public Service, special requirements and additional requirements) shall be determined by this Law and a respective legal act of the Head of the Personal Data Protection Service. In order to hold a competition for the selection and appointment of an employee of the structural unit carrying out an official inspection of the Personal Data Protection Service, the Head of the Personal Data Protection Service shall establish a competition commission and determine the rules for its operation.
2. An employee of the structural unit carrying out an official inspection of the Personal Data Protection Service may be transferred, without a competition, to another institution based on the principle of mobility, or through a horizontal transfer, as provided for by the Law of Georgia on Public Service.
3. The powers and duties determined by this Law and a respective legal act of the Head of the Personal Data Protection

Service shall apply to an employee of the structural unit carrying out an official inspection of the Personal Data Protection Service.

Chapter IX – Procedures for Carrying out Proceedings, Reviewing Administrative Offences and Imposing Administrative Penalties

Article 58 – General provisions for carrying out proceedings by the Personal Data Protection Service

1. Administrative offences related to processing personal data as provided for by Articles 66-87 of this Law ('an administrative offence') shall be identified and the respective administrative liability shall be imposed based on the checking (inspection) carried out by the Personal Data Protection Service, and/or the review of an application of a data subject ('the proceedings'). An administrative offence report shall be drawn up and a respective administrative penalty shall be imposed on an offender by the Personal Data Protection Service according to the procedure established by the legislation of Georgia.
2. Based on a decision of the Head of the Personal Data Protection Service, it is permissible to combine more than one proceedings into one case, or to separate a case from the proceedings.
3. The powers of the Head of the Personal Data Protection Service and the procedure for carrying out the proceedings shall be determined by this Law, the Administrative Offences Code of Georgia, other legislative acts, and the normative acts of the Head of the Personal Data Protection Service.
4. In the case of any interrelation between the norms of the Administrative Offences Code of Georgia and of this Law, the norms of this Law shall prevail.

Article 59 – Evidence

1. For the purposes of proceedings, evidence is all actual data, based on which the Head and/or an authorised person of the Personal Data Protection Service shall, according to the procedure established by the legislation of Georgia, establish the existence or otherwise of an administrative offence, a person's culpability in committing such an offence, and other circumstances that are of importance for the correct resolution of the case.
2. For the purposes of this article, the following may be considered as evidence: information and documents obtained as a result of the review of an application of a data subject and/or the checking (inspection); the explanations of a data subject, a controller, a joint controller, a processor, a special representative, and a witness; an offender's confession; minutes of an oral session (recording); an expert opinion; fact-finding materials; an audio recording; a video recording; a photo; information and documents obtained from public sources; a document prepared/issued/certified by an authorised person or body; an administrative offence report drawn up by the Head or an authorised person of the Personal Data Protection Service, the form of and procedure of acquainting with which shall be determined by the Head of the Personal Data Protection Service; a report for checking (inspecting) the lawfulness of data processing; material evidence; any other information, document or material that is of importance in establishing the objective circumstances of a case.

Article 60 – Circumstances to be established during the proceedings and imposition of an administrative penalty

1. In the course of reviewing cases of administrative offences and imposing an administrative penalty, the Personal Data Protection Service or a court shall establish whether an administrative offence has been committed, whether a person is guilty of committing it, whether such person is subject to administrative liability, whether any circumstances mitigating or aggravating administrative liability are present, as well as other circumstances that are of importance for the correct resolution of a case.
2. If there are any circumstances mitigating administrative liability, the Personal Data Protection Service or a court shall be authorised to issue a warning to an offender in the case of a minor administrative offence.
3. An administrative penalty for committing an administrative offence shall be imposed on an offender within the scope determined by this Law, in accordance with the article that provides for administrative liability.

Article 61 – Circumstances mitigating liability for an administrative offence

1. The following circumstances shall be considered as mitigating the administrative liability for an administrative offence:
a) terminating an unlawful act and remedying the damage caused as a result of the administrative offence, and/or taking appropriate organisational and technical measures for the prevention of similar offences in the future;
b) the commission of an administrative offence by a minor;
c) the sincere repentance of an administrative offence and cooperation with the Personal Data Protection Service;
d) other circumstances, such as the nature of the administrative offence and the degree of charges against the offender, which are considered as mitigating circumstances by the Head of the Personal Data Protection Service during the resolution of the case.
2. The obligation to submit evidence of the existence of circumstances mitigating administrative liability determined by paragraph 1 of this article shall rest with a controller/processor.
3. If there are any mitigating circumstances as provided for by paragraph 1(a) and/or (b) of this article, the amount of fines determined by Articles 66-87 of this Law shall be reduced by 30 per cent.

4. If there are any mitigating circumstances as provided for by paragraph 1(c) and/or (d) of this article, the amount of fines determined by Articles 66-87 of this Law shall be reduced by 20 per cent.
5. In the case of the simultaneous existence of grounds for reducing the amount of fines under paragraphs 3 and 4 of this article, the amount of fines determined by Articles 66-87 of this Law shall be reduced by 50 per cent.

Article 62 – Circumstances aggravating liability for an administrative offence

The following circumstances shall be considered as aggravating administrative liability for the administrative offences provided for by this Law:
a) the repeated commission of the same administrative offence within 1 year, for which an administrative penalty has already been imposed on a controller/processor/third party;
b) processing large quantities of data subjects' data in violation of the requirements of this Law, or a risk thereof;
c) processing minors' data in violation of the requirements of this Law;
d) the commission of an administrative offence for financial or other gain;
e) the commission of an administrative offence on the grounds of discrimination.

Article 63 – Right to appeal a decision of the Head of the Personal Data Protection Service made as a result of the proceedings

1. A decision made by the Head of the Personal Data Protection Service as a result of the proceedings may be appealed before a court, according to the procedure established by the Administrative Offences Code of Georgia, by a person, against whom such decision has been made, within 1 month after the official notification of such decision.
2. If a decision made by the Head of the Personal Data Protection Service as a result of the proceedings is appealed before a court, it shall be enforced from the moment the decision of the court enters into legal force.

Article 64 – Imposition of an administrative penalty for committing several administrative offences

1. If a person commits multiple administrative offences, the total amount of fines imposed on the person shall not exceed the amounts provided for by paragraph 2 of this article, if any of the following conditions is met:
a) the administrative offences have been identified as a result of a single checking;
b) the issue of imposition of administrative liability for several administrative offences is examined within the framework of a single set of proceedings;
c) administrative liability is imposed for the administrative offence that had been committed before the imposition of an administrative penalty already applied against the same person, in which case both the amount of imposed administrative liability and the amount of the administrative liability to be imposed shall be taken into account.
2. In the case provided for by paragraph 1 of this article, the total amount of fines imposed on a person shall not exceed:
a) GEL 10 000 in the case of a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) GEL 20 000 in the case of a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
3. If the same action can be qualified as several administrative offences determined by the respective articles of this Law, administrative liability shall be imposed only for the administrative offence and within the scope for which the heaviest liability is provided for by this Law.
4. For the purposes of paragraph 3 of this article, a violation shall be considered as a single action even if it constitutes a combination of several actions closely and directly related to one another, which amount to essentially a single administrative offence.
5. If only one joint controller is guilty of committing an administrative offence provided for by this Law, an administrative penalty shall be imposed only on him/her/it, and if simultaneously more than one joint controllers are found guilty, an administrative penalty shall be imposed on the offending joint controllers jointly and severally.
6. In the case of the commission of an administrative offence provided for by this Law, other measures determined by Article 52 of this Law may also be applied together with an administrative penalty.
7. The Head of the Personal Data Protection Service shall be authorised, for the purposes of the imposition of administrative liability under this Law, to request and receive from the LEPL Revenue Service information on the annual turnover of a legal person, a branch of a foreign enterprise, and an individual entrepreneur, as well as to have access to the relevant electronic database of the LEPL Revenue Service.

Article 65 – Timeframe for imposing an administrative penalty

1. Liability may be imposed on a person for committing an administrative offence provided for by this Law within not later than 4 months from the date of the commission of the administrative offence, and if the offence is continuing, within not later than 4 months from the date of its identification.
2. If a criminal prosecution or an investigation has been terminated but there are elements of administrative offence in the actions of an offender, an administrative penalty may be imposed on the offender within not later than 2 months from

the date the decision on the termination of the criminal prosecution or investigation was made.
3. If a decision made regarding an administrative offence is appealed before a court, the running of the timeframe for the imposition of an administrative penalty provided for by paragraph 1 of this article shall be suspended until the court delivers a final decision on the case.

Chapter X – Administrative Offence and Administrative Liability

Article 66 – Violation of the principles of data processing

1. The violation of any principle of data processing provided for by this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. The violation of two or more principles of data processing provided for by this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
3. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 1 500 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
4. An act provided for by paragraph 2 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 67 – Processing data without the grounds provided for by this Law

1. Processing data without the grounds provided for by this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 68 – Processing special category data without the grounds provided for by this Law

1. Processing of special category data without the grounds provided for by this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-

entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 69 – Violation of the rules for video monitoring or audio monitoring

1. The violation of the rules of video monitoring determined by Article 10 of this Law (except for the cases provided for by paragraphs 2 and 4 of this article) or of the rules of audio monitoring determined by Article 11 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. Carrying out video monitoring in changing rooms, hygiene facilities, or other places, where a data subject has a reasonable expectation of protection of privacy and/or where the carrying out of surveillance contradicts universally recognised moral norms, –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
3. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
4. An act provided for by paragraph 2 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 70 – Violation of the rules for processing the data of deceased persons

1. Processing the data of a deceased person in violation of Article 8 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial)

legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 71 – Processing data for the purposes of direct marketing in violation of rules

1. Processing data for the purposes of direct marketing in violation of the rules established by this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 4 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 6 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 72 – Violation of the rights of a data subject as provided for by Chapter III of this Law

1. The violation of any right of a data subject provided for by Chapter III (except for Article 22) of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 1 500 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. The violation of two or more rights of a data subject provided for by Chapter III (except for Article 22) of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
3. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 1 500 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
4. An act provided for by paragraph 2 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 73 – Failure to comply with the obligations provided for by Article 21(2) and (4) of this Law

1. The failure to comply with the obligation provided for by Article 21(2) of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;

b) the issuance of a warning to or the imposition of a fine of GEL 1 500 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. The failure to comply with the obligation provided for by Article 21(4) of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 1 500 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
3. An act provided for by paragraph 1 or 2 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 74 – Failure to comply with the obligation to inform a data subject
1. The failure to comply with the obligation to inform a data subject as provided for by Articles 24 and 25 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 1 500 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 75 – Violation of the requirement of data masking priority as an initial method used automatically before choosing an alternative approach when creating a new product or service
1. The failure to comply with any of the obligations determined by Article 26 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 76 – Failure to comply with the obligation to ensure data security
1. The failure to comply with the obligation, as provided for by this Law, to ensure data security determined by Article 27 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual

entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 77 – Failure to comply with the obligation to register information related to data processing
1. The failure to comply with the obligation, as provided for by this Law, to register information related to data processing under Article 28 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 1 500 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 78 – Failure to comply with the obligation to notify the Personal Data Protection Service of an incident
1. The failure to comply with the obligation to notify the Personal Data Protection Service of an incident as provided for by Article 29 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 79 – Failure to comply with the obligation to inform a data subject of an incident
1. The failure to comply with the obligation to inform a data subject of an incident as provided for by Article 30 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:

a) the imposition of a fine of GEL 5 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 10 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 80 – Failure to comply with the obligation to carry out a data protection impact assessment
1. The failure to comply with the obligation to carry out a data protection impact assessment as provided for by Article 31 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 3 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 81 – Failure to comply with the obligations, as provided for by the law, in the course of obtaining the consent of a data subject and the withdrawing of consent by a data subject
1. The failure to comply with the obligations, as provided for by this Law, in the course of obtaining the consent of a data subject and the withdrawing of consent by a data subject under Article 32 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 82 – Failure to comply with the obligation to appoint a personal data protection officer
1. The failure to comply with the obligation to appoint a personal data protection officer as provided for by Article 33(1) of this Law –
shall result in the issuance of a warning to the offender.
2. The failure by a personal data processor/processor to comply with the obligation to appoint a personal data protection officer as provided for by Article 33(1) of this Law within 1 year after the imposition of an administrative penalty by the Head of the Personal Data Protection Service –
shall result in the imposition of a fine of GEL 3 000 on the offender.

Article 83 – Failure to comply with the obligation to designate/appoint a special representative
1. The failure by a controller to comply with the obligation to designate/appoint a special representative as provided for by Article 34(1) of this Law –
shall result in the issuance of a warning to or the imposition of a fine of GEL 3 000 on the offender.
2. The failure to comply with the obligation to designate/appoint a special representative as provided for by Article 34(1) of this Law within 1 year after the imposition of an administrative penalty by the Head of the Personal Data Protection Service –
shall result in the imposition of a fine of GEL 5 000 on the offender.

Article 84 – Failure to comply with the obligations provided for by Articles 35 and 36 of this Law

1. The failure by a controller/processor to comply with the obligations provided for by Articles 35 and 36 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 85 – Violation of the rules established by Article 37 of this Law

1. The transfer of data to another state and/or an international organisation in violation of the rules established by Article 37 of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

2. An act provided for by paragraph 1 of this article, committed with an aggravating circumstance (circumstances), –
shall result in:
a) the imposition of a fine of GEL 4 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 6 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 86 – Obstructing the Head or an authorised person of the Personal Data Protection Service to exercise rights provided for by this Law

1. The violation of the rules for providing information and/or documents under Article 51(3) of this Law, or the provision of false information, to the Head or an authorised person of the Personal Data Protection Service –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

2. The same act committed by a person on whom an administrative penalty has been imposed in the course of 1 year for committing an offence provided for by paragraph 1 of this article –
shall result in:
a) the imposition of a fine of GEL 3 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 5 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

3. Obstructing, in any form, the Personal Data Protection Service or an authorised person of the Personal Data Protection Service from exercising the right provided for by Article 51(6) of this Law –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual

entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 4 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.
4. The same act committed by a person on whom an administrative penalty has been imposed in the course of 1 year for committing an offence provided for by paragraph 3 of this article –
shall result in:
a) the imposition of a fine of GEL 4 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the imposition of a fine of GEL 6 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Article 87 – Failure to comply with a lawful request of the Personal Data Protection Service

The failure to comply with a lawful request of the Personal Data Protection Service (in accordance with Article 51(1)(a)-(d) of this Law) –
shall result in:
a) the issuance of a warning to or the imposition of a fine of GEL 1 000 on a natural person, public institution, non-entrepreneurial (non-commercial) legal entity, as well as a legal person, a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover does not exceed GEL 500 000;
b) the issuance of a warning to or the imposition of a fine of GEL 2 000 on a legal person (except for non-entrepreneurial (non-commercial) legal entities), a branch of a foreign enterprise, and an individual entrepreneur, whose annual turnover exceeds GEL 500 000.

Chapter XI – Transitional and Final Provisions

Article 88 – Transitional provisions

1. Before 1 March 2024, administrative liability shall be imposed on an offender for committing an administrative offence related to the processing of personal data in accordance with the Law of Georgia on Personal Data Protection of 28 December 2011.
2. A controller/processor shall be exempted from the obligations provided for by Article 10(9) and Article 11(4) of this Law with respect to warning signs placed before 1 March 2024.
3. A controller shall be exempted from the obligation provided for by Article 26 of this Law with respect to software used for data processing and developed before 1 March 2024, unless the software has been significantly updated after 1 March 2024 and the compliance with the obligation provided for by the same Article does not require the controller to incur unreasonable expenses.
4. Before 1 March 2024, the Head of the Personal Data Protection Service shall issue the following normative acts:
a) the criteria for determining incidents posing a significant threat to fundamental human rights and freedoms, and the procedure for notifying the Personal Data Protection Service of an incident. This normative act shall be issued in agreement with the relevant state agencies;
b) on the criteria for determining the circumstances giving rise to the obligation for a data protection impact assessment, and the assessment procedure;
c) on determining the category of persons who are not obliged to designate/appoint a personal data protection officer;
d) the procedure for registering a special representative by the Personal Data Protection Service.

Article 89 – Invalidated normative acts

The Law of Georgia on Personal Data Protection of 28 December 2011 shall be declared invalid (Legislative Herald of Georgia (www.matsne.gov.ge), 16.1.2012, registration code: 010100000.05.001.016606).

Article 90 – Entry into force of the Law

1. This law, except for Articles 1-87, Article 88(2) and (3) and Article 89 of this Law, shall enter into force upon its promulgation.
2. Articles 1-5, Article 6(1)(a)-(q), (2) and (3), Articles 7-30, Article 32, Articles 34-79, Article 81, Articles 83-87, Article 88(2) and (3), and Article 89 of this Law shall enter into force on 1 March 2024.
3. Articles 31, 33, 80 and 82 of this Law shall enter into force on 1 June 2024.
4. Article 6(1) (s) of this Law shall enter into force on 1 January 2025.
5. Article 6(1) (r) of this Law shall enter into force on 1 January 2027.
Law of Georgia No 4406 of 5 September 2024 – website, 23.9.2024

President of Georgia **Salome Zourabichvili**

Tbilisi
14 June 2023
No 3144-XI ᲛᲑ -X ᲛᲓ