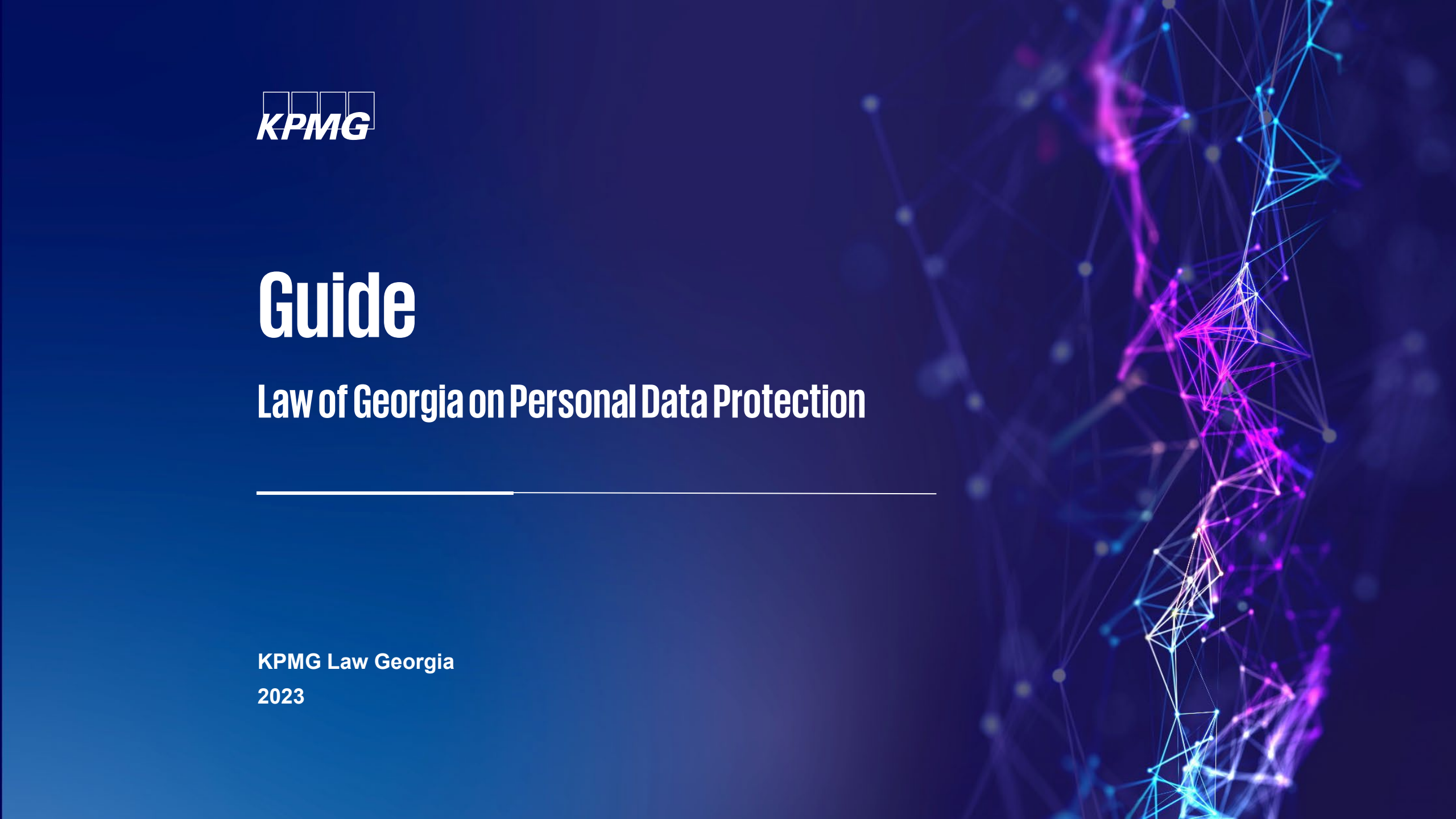


Guide

Law of Georgia on Personal Data Protection

KPMG Law Georgia

2023

Contents

Introduction

Nowadays, it is rare to find an organization that does not handle or otherwise deal with personal data. Regardless of the industry or product, the collection, storage and use of information about customers, employees and partners is a widespread practice. Respectively, all organizations or individuals who interact with personal data have their own role in this process, entailing corresponding rights and responsibilities.

Globally, the manner in which companies process data has undergone significant changes since May 25, 2018, when the General Data Protection Regulation (GDPR) came into force. GDPR completely transformed issues related to personal data, established new standards for data protection, and introduced novel concepts and institutions concerning the security and use of personal data.

It should be noted that, although Georgia is not a member of the European Union, GDPR still indirectly applies to Georgia. Organizations not registered in the EU but processing the data of individuals in the European Union fall within the scope of the GDPR.

GDPR has, to a certain extent, become an international standard for personal data protection. Consequently, Georgia aims to align local legislation to it.

On 14 June, 2023, the Parliament of Georgia adopted a new law "On Personal Data Protection" (the "Law"), which completely changed the existing version of the law. The Law not only establishes new standards for personal data protection, but also introduces additional principles and obligations that organizations must adhere to when processing such data. Clearly, such fundamental changes represent a significant challenge for anyone dealing with personal data. These organizations must address questions such as when, how, and on what basis process personal data. They also need to consider whether updates to technical, organizational, and/or business practices are necessary. It is important to note that organizations failing to ensure the protection of personal data and compliance with the new regulations are exposed not only to the risk of financial fines but also the risk of reputational loss.

> **Organizations failing to ensure the protection of personal data and compliance with the new regulations are exposed not only to the risk of financial fines but also the risk of reputational loss.**

What is personal data?

Personal data represents **any information**, which allows to **identify** a natural person. In turn, a natural person can be identified in two ways:

Directly

When specific data (e.g. name, surname, date of birth or personal number) exclusively identifies the person.

Indirectly

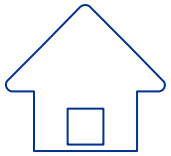
When by combining various information (e.g. location, workplace and job title) it is possible to identify a specific person.

Some personal data fall under **special categories** of data and their processing requires additional guarantees and more solid processing grounds. Special categories of data involve sensitive information. Improper use of such data can cause a significant harm to the individual. Examples of special categories of personal data may include, but are not limited to:

- Person's racial or ethnic origin
- Political views
- Religious, philosophical or other beliefs
- Genetic data
- Biometric data
- State of health
- Sexual life
- Membership of professional unions

Examples of personal data


Name, surname


Residential address


E-mail address


Marital status

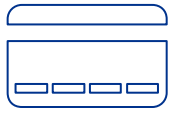

Fingerprint


Photo


Blood type


Conviction


Remuneration


Card number


Telephone number


Date of birth

What does personal data processing mean?

The term "processing" has a rather broad meaning and refers to any actions taken with respect to the data, inter alia:

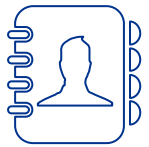
- Collecting, obtaining, accessing, photographing
- Video recording, audio recording
- Organizing, grouping, interconnecting
- Storing, altering, retrieving, requesting for access, using, locking, erasing, or destroying
- Disclosing by transmission, publication, dissemination or otherwise making available

Data is processed by the following methods:

Automated data processing

Processing data by means of information technologies.

For example: processing certain data by computer.



Data processing by non-automatic means

Processing data without using information technologies.

For example: when the whole process is managed manually, without technological interventions.

Principles of data processing

Data should be processed according to the following **principles:**

- Lawfulness, fairness, transparency, protection of the dignity of the data subject
  For example: Organization is required to provide the data subject with a comprehensive disclosure regarding the data intended for processing.
- The existence of a specific, clearly defined and legitimate purpose
  For example: If the data is processed for one specific purpose, it must not be processed for another, incompatible reason.
- Proportionality and processing only the necessary data
  For example: If only the subject's phone number and e-mail address are necessary to achieve a specific purpose, other data (for example: personal number) should not be processed.
- Ensuring the validity and accuracy of the data and, if necessary, keeping the data up-to-date
  For example: If the telephone number of the data subject is processed, it should be updated whenever the data subject changes the number.
- Storing the data only for the period necessary to achieve a legitimate purpose
  For example: If to achieve a certain purpose data processing was required for 2 days, it is not allowed to process and store data for a longer period of time. After the expiration of the mentioned period, the data should be immediately deleted or destroyed or stored in a form which does not allow the identification of a person.
- The existence of appropriate technical and organizational measures during processing
  For example: If the existence of specific and/or updated technical means is necessary for the security of the data, the data should be processed through these means.

Recommendations

- Organization shall establish internal policies which determine in advance what type of data, for what period and on what grounds is processed and stored.
- Appropriate communication channel shall be established with the data subjects, providing them with the opportunity to express their opinions and/or seek information concerning their data.
- Appropriate technical and organizational checks and analysis shall be carried out to ensure maximum data protection, prior to data processing.

Grounds for data processing

One of the following **grounds** is required for data processing:

- Consent of the data subject
- Fulfillment of contractual obligations with data subject
- Processing is provided for by law
- Data is publicly available
- To protect vital and/or public interests
- Data processing is necessary for a data controller to perform its statutory duties
- To protect significant legitimate interests
- To deal with the data subject’s application

Consent

Consent is one of the most common grounds for data processing. The Law sets clear requirements in this regard, particularly:

- Prior to obtaining consent, the subject should be provided with complete information on what data will be processed, for what purpose and for what period
- Consent should be expressed with active actions, in written or oral forms
- Consent should be based on the free and clear expression of the individual's will
- The data subject should have the right to withdraw his/her consent at any time, without any reason or explanations, and the withdrawal procedure should be as simple as expressing the consent

Grounds for data processing

It is important to highlight that the Law approaches special category data with greater caution, and imposes stricter requirements. For instance, when it is necessary to secure the data subject's consent for data processing, written consent is mandatory for the processing of special category data. The Law has different requirements in the following cases:

Minors	Deceased person	Biometric	Direct Marketing	Video monitoring	Audio monitoring
The ground for processing minor's data (under the age of 16) requires consent of the parent or legal representative, or in case of a minor over the age of 16 - his/her own consent. This rule does not apply to special category data of a minor, the processing of which requires consent of a parent or a legal representative.	The data on a deceased person may be processed based on: (i) the grounds for processing the relevant data; (ii) if data processing is not prohibited by the parent, child, grandchild or spouse of the data subject; (iii) 30 years have passed since the death of the data subject; (iv) data processing is necessary to realize inheritance rights.	Biometric data may be processed only in cases provided for by Law (e.g. for the purposes of crime investigation, to provide human safety and property protection, also to prevent disclosure of secret information, if these goals may not be reached by other means or require unjustifiably great efforts).	If an organization directly offers goods, ideas, services or communicates other matters as determined in the Law by telephone calls, mail, e-mail or other means of communication, the data on the data subject may be processed only with the consent of the data subject.	Video recording of the territory with a surveillance system installed in public or private spaces is allowed only in cases provided for by the Law, if the goal (including, but not limited to: protection of safety and property, control of examination/testing process) cannot be achieved by other means or if this requires disproportionately great efforts.	Audio recording with a surveillance system installed in public or private spaces is allowed: in cases directly provided for by the Law and/or if there is a consent of the data subject and/or to produce a recording notice and/or to protect the legitimate interest of the data controller (person responsible for data processing).

Participants

The Law on Personal Data Protection applies to:

Any person carrying out data processing on the territory of Georgia.

Persons registered outside Georgia, but who carry out data processing by using technological resources existing on the territory of the Country.

Special Representative

The data controller/data processor, registered outside of Georgia but utilizing technical means existing in Georgia for data processing, is obliged to appoint or designate a special representative in Georgia before commencing the data processing.

- The special representative is registered by the Personal Data Protection Service.
- The data controller/data processor has the right to process data only after the registration of the special representative.
- It is not necessary to appoint a special representative, if (a) the person is registered in the member state of the EU or if (b) the person is registered in the state with adequate data protection recognized by the EU.

Participants

- Data subject
  Any natural person whose data is being processed.

- Data controller*
  Data controller is any natural person, organization, or public institution that determines the purposes and means of processing personal data, either individually or through others. The data controller is responsible for making decisions regarding which information to receive, the reasons for receiving it, the methods of processing, and the duration for which it will be processed.

- Data processor*
  Data processor is any natural person, organization, or public institution, which processes data for or on behalf of the data controller. Data processor may process data only based on: (a) legal act or (b) a written agreement with the data controller.

- Joint controllers
  If the data is processed by two or more persons i.e. they jointly determine the purposes and means of processing, then these persons are called joint controllers. The joint controllers are required to define their rights and obligations in advance, in writing. This information should be available to the data subjects.

The following example illustrates the difference between the data controller and the data processor:

A confectionery based in Georgia receives personal data from data subjects (e.g., name, surname, telephone number, address) to provide services within the territory of Georgia. The confectionery, in turn, has an agreement with delivery service companies to which it transfers information regarding the orders for delivery.

In the example above, the confectionery acts as the data controller, while the delivery service company functions as the data processor.

Rights of the data subject

The Law grants broad powers to the data subjects, enabling them to play an active role in the processing. Data subjects have following rights:

To be informed

In order to realize this right, the data subject may request information on who, how, by what means and for what period of time processes his/her personal data and what guarantees, and protection measures are taken to protect this information. Data subject may also request to get acquainted with the data about him/her and receive respective copies.

To request data correction

To ensure that the data is accurate, correct, and up-to-date, the Law provides the data subject with the right to request the correction, update, or addition of any information that is found to be incorrect, inaccurate, or incomplete.

To prohibit data processing

To emphasize the fact that the data subject has control over the information on him/her, the Law grants the data subject the right to request to stop processing and delete or destroy the information on him/her. According to GDPR, this right of the data subject is called - "right to be forgotten", which reflects the purpose of this right.

To revoke consent

One of the most common grounds for data processing is the consent of the data subject. Accordingly, the data subject has the right to revoke his/her own consent without any additional effort, explanation, or reasoning.

To appeal violation

If the data subject believes that his/her rights have been violated, he/she has the right to address the relevant authorities (Personal Data Protection Service, higher administrative bodies and/or courts) and request the restoration of the violated right(s).

Limitations

While the data subject is the controller of his/her information, the Law imposes certain restrictions. In specific instances, such as the right to revoke consent, certain rights of the data subject may be limited. The basis for restricting the data subject's rights is strictly defined by the Law. Such restrictions are considered permissible only to the extent necessary to achieve the purpose outlined in the Law for the restriction.

Obligations of the processor/controller

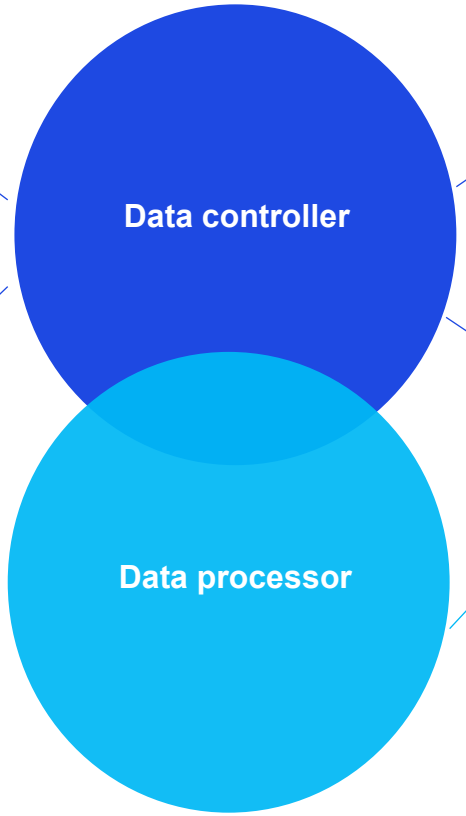
The data controller/processor shall process information according to the principles determined by the Law and respective processing grounds, ensure the realization of the rights of the data subject and take all measures necessary to protect the data. For this purpose, the Law distinguishes between the obligations of the data controller and the data processor.

Informing the data subject

If the information is collected directly from the data subject, he/she should be informed on who collects the data, by what means, on what grounds, for what period of time and what type of data is collected. If the data is not collected directly from the data subject, the source of the information should be indicated.

Recording obligation

Information about person processing the data, its purpose, data subject and period of processing as well as technical and organizational measures applied for protection of data should be recorded. Same applies to the permissions issued by the Personal Data Protection Service if international data transfer takes place.



Consent revocation mechanism

One of the grounds for data processing is the consent given by the data subject, which can be revoked by the data subject himself/herself. The processor is obliged to develop such mechanism that the data subject can easily, without any complications, exercise his/her right to revoke his/her consent.

Ensuring security

To ensure the security of the data, and avoid all possible risks that could endanger data protection, the appropriate organizational and technical measures should be taken. Given that the technologies are constantly evolving, the Law obliges the data processor to periodically review the protection mechanisms and update them, if necessary.

Obligations of controller

The Law introduced several important obligations for data controllers, including:

Data protection impact assessment

A preliminary assessment in written form is mandatory if (i) there is a high risk of endangering basic human rights and freedoms; (ii) decisions related to the subject's legal, financial, or other matters of material significance are made on automated basis in the organization; (iii) if a large volume of the subject's special category data is being processed; (iv) if there is systematic and large-scale monitoring of the subject's behavior in places of public gathering. If the assessment reveals that the basic human rights and freedoms are at high risk, data controller is obliged to take all measures to reduce this risk, and also has the right to address Personal Data Protection Service for consultation. If appropriate organizational and technical improvements cannot reduce the risk, the processing should not take place.

The obligation to record and react to the incident

If the data security has been breached, the data controller is obliged to:

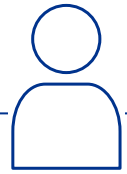
- Record the incident, the resulting outcome and the measures taken;
- Report the incident to the personal data protection service within 72 hours;
- Without delay, in plain language, notify the data subject of the incident, unless there are circumstances precluding notification.

Data protection by design and by default

At the initial stages, the processor should develop such technical and organizational measures, which ensure the protection and maximum transparency of the data. For this purpose, the processor must ensure the implementation of such a system, which provides the following guarantees at the initial stages:

- Processing only such amount of data, which is necessary to achieve the intended purpose.
- The identification of data shall be impossible, more precisely, the data shall be stored in an encrypted form (including, using pseudonymization and other encryption methods), which shall make it impossible to connect the data and the data subject and to identify the data subject.

Obligations of the controller/processor



Personal data protection officer

The processors are obliged to appoint personal data protection officer:

- If they process large volume of personal data
- If they carry out systematic and large-scale monitoring of the data subject's behavior

Or if they represent:

- Public institution
- Insurance company
- Commercial bank
- Microfinance organization
- Credit bureau
- Electronic communications company
- Airline
- Airport
- Medical institution

Personal data protection officer ensures:

- Notifying organization and its employees of data protection issues;
- Developing internal regulations and documents and monitoring their implementation;
- Analyzing the applications and complaints received in the organization and issuing appropriate recommendations;
- Cooperation with personal data protection service;
- Notifying data subject of data processing and procedures.

Information

Data protection officer may be:

- An employee of the organization
- A person determined by the service agreement

The data controller and the data processor can designate a common data protection officer.

The data controller and the data processor are obliged to inform the personal data protection service (which publishes such information) of the identity and contact information of the personal data protection officer within 10 working days of his/her appointment or designation, or replacement.

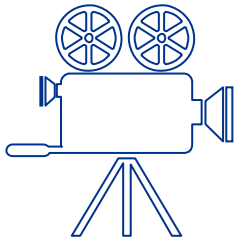
Data controller and data processor are obliged to proactively publish the identity and contact information of the personal data protection officer on the website (if any) or by other available means.

Video and audio monitoring

Grounds for video and audio monitoring processing grounds have already been explained above. However, given the sensitivity of the data processed through the means, the Law sets additional limitations for processors.

In both cases, it is mandatory:

- For the controller to determine in advance, in written form, the purpose, volume, duration, access, storage, destruction rules and conditions of monitoring, data subject protection mechanisms.
- To place warning sign in a visible place about the progress of video/audio monitoring, which should contain the following information: a simple and understandable image of video/audio monitoring and the name and contact data of the person responsible for processing.



Video monitoring

- The monitoring of a residential building is allowed only if: the common entrance and common space are being monitored and there is a written consent of more than half of the owners.
- Video monitoring is not allowed in changing rooms and hygiene areas.
- The working space may be monitored only in exceptional cases.
- The controller/processor is obliged to pay special attention to the materials obtained as a result of video monitoring and is obliged to record every case of access to video recordings.

Audio monitoring

- Before the start of audio monitoring, the controller/processor should warn the person in advance about the progress of monitoring. Also, shall explain that the person has the right to refuse.

Direct marketing and international transfer

Data processing for direct marketing purposes

Today, offering services or products via telephone or electronic mail is one of the most established methods, involving the processing of data for dozens of subjects.

As mentioned earlier, the processing of data for direct marketing purposes occurs only with the consent of the data subject. Consequently, it is crucial for the processor/controller to establish a system customized for the data subject, ensuring that the process of revoking consent is straightforward and comprehensible. The processor/controller is obliged to record the time and the fact of giving, as well as revoking, the consent by the data subject.

Key note:

- Data processing should be terminated as soon as possible after the revocation of the consent, no later than within 7 days.
- The right to withdraw consent is free of charge and may not be subject to any fees or restrictions.
- The processor is obliged to store this information for the duration of direct marketing or for 1 year after the termination.

International transfer of personal data

Transfer of personal data to another state and international organization means transferring or sharing data from the territory of Georgia to another jurisdiction.

For example, if a travel agency based in Georgia utilizes a third-party platform located in another country to manage reservations, international transfer of personal data takes place when the customer's personal data, provided for booking, is transmitted from Georgia to another country.

Before the international transfer of data, it is important that the organization asks the following questions, and only in case of a positive answer to any of them, transfers the data internationally according to the rules established by the Law:

- Is data transfer provided for by the international treaty or agreement?
- Are adequate data protection safeguards in place?
- Is there a written consent of the data subject?
- Is data transfer necessary to protect vital interests?
- Is there a significant public interest?

Sanctions

The violation of the requirements of the Law may result in number of sanctions, the nature and amount of which depends on the nature and severity of the violation. Violations related to personal data processing are detected and appropriate liability is imposed by the Personal Data Protection Service.

NNLE - Non-entrepreneurial Non-commercial Legal Entity

I/E - Individual Entrepreneur

	Natural person	State authority	N(N)LE	Legal person	Branch	I/E	Legal person	Branch	I/E
				Annual turnover < GEL 500,000			Annual turnover > GEL 500,000		
Violation of data processing principles									
Violation of one principle	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
Violation of one principle (in the presence of aggravating circumstance(s))	Fine GEL 1,500						Fine GEL 3,000		
Violation of two or more principles	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Violation of two or more principles (in the presence of aggravating circumstance(s))	Fine GEL 3,000						Fine GEL 4,000		
Data processing without processing grounds									
Without grounds	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
Without grounds (in the presence of aggravating circumstance(s))	Fine GEL 2,000						Fine GEL 4,000		
Special category data processing without processing grounds									
Without grounds	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Without grounds (in the presence of aggravating circumstance(s))	Fine GEL 3,000						Fine GEL 5,000		
Violation of the rules of video monitoring or audio monitoring									
Violation of the rules of video monitoring or audio monitoring	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		

Sanctions

	Natural person	State authority	N(N)LE	Legal person	Branch	I/E	Legal person	Branch	I/E
				Annual turnover < GEL 500,000			Annual turnover > GEL 500,000		
Violation of the rules of video monitoring or audio monitoring (in the presence of aggravating circumstances)	A warning or a fine of GEL 2,000						A warning or a fine of GEL 4,000		
Video monitoring in changing rooms, areas designated for hygiene or other spaces where the subject has a reasonable expectation of protection of personal life and/or monitoring is against the generally accepted moral norms	A warning or a fine of GEL 3,000						A warning or a fine of GEL 5,000		
Video monitoring in changing rooms, areas designated for hygiene or other spaces where the subject has a reasonable expectation of protection of personal life and/or monitoring is against the generally accepted moral norms (in the presence of aggravating circumstances)	Fine GEL 3,000						Fine GEL 5,000		
Violation of data processing rules of a deceased person									
Violation of data processing rules of a deceased person	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
Violation of data processing rules of a deceased person (in the presence of aggravating circumstances)	Fine GEL 2,000						Fine GEL 4,000		
Data processing for direct marketing purposes in violation of the rules									
Data processing for direct marketing purposes in violation of the rules	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Data processing for direct marketing purposes in violation of the rules (in the presence of aggravating circumstances)	Fine GEL 4,000						Fine GEL 6,000		

Sanctions

	Natural person	State authority	N(N)LE	Legal person	Branch	I/E	Legal person	Branch	I/E
				Annual turnover < GEL 500,000			Annual turnover > GEL 500,000		
Violation of the rights of the data subject									
Violation of any of the rights of the data subject	A warning or a fine of GEL 1,000						A warning or a fine of GEL 1,500		
Violation of any of the rights of the data subject (in the presence of aggravating circumstance(s))	Fine GEL 1,500						Fine GEL 3,000		
Violation of two or more rights	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Violation of two or more rights (in the presence of aggravating circumstance(s))	Fine GEL 3,000						Fine GEL 5,000		
Failure to fulfill the obligation to inform									
Failure to fulfill the obligation to inform	A warning or a fine of GEL 1,000						A warning or a fine of GEL 1,500		
Failure to fulfill the obligation to inform (in the presence of aggravating circumstances)	Fine GEL 2,000						Fine GEL 3,000		
Data protection by default and by design									
Failure to fulfill the obligation	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 3,000						Fine GEL 5,000		
Failure to fulfill data security obligation									
Failure to fulfill the obligation	A warning or a fine of GEL 2,000						A warning or a fine of GEL 4,000		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 3,000						Fine GEL 5,000		

Sanctions

	Natural person	State authority	N(N)LE	Legal person	Branch	I/E	Legal person	Branch	I/E
				Annual turnover < GEL 500,000			Annual turnover > GEL 500,000		
Failure to fulfill the obligation to record information									
Failure to fulfill the obligation	A warning or a fine of GEL 1,000						A warning or a fine of GEL 1,500		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 2,000						Fine GEL 3,000		
Failure to report the incident to the inspector									
Failure to fulfill the obligation	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 3,000						Fine GEL 5,000		
Failure to report the incident to the data subject									
Failure to fulfill the obligation	A warning or a fine of GEL 3,000						A warning or a fine of GEL 5,000		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 5,000						Fine GEL 10,000		
Failure to fulfill impact assessment obligation									
Failure to fulfill the obligation	A warning or a fine of GEL 2,000						A warning or a fine of GEL 3,000		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 3,000						Fine GEL 5,000		

Sanctions

	Natural person	State authority	N(N)LE	Legal person	Branch	I/E	Legal person	Branch	I/E
				Annual turnover < GEL 500,000			Annual turnover > GEL 500,000		
Acceptance and withdrawal of consent									
Failure to fulfill the obligation	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
Failure to fulfill the obligation (in the presence of aggravating circumstances)	Fine GEL 2,000						Fine GEL 4,000		
Joint controllers									
Failure to fulfill the obligations determined by the law	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
Failure to fulfill the obligation determined by the law (in the presence of aggravating circumstances)	Fine GEL 2,000						Fine GEL 4,000		
Data processor									
Failure to fulfill the obligations determined by the law	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
Failure to fulfill the obligation determined by the law (in the presence of aggravating circumstances)	Fine GEL 2,000						Fine GEL 4,000		
Data transfer to another state and/or international organization									
Transfer in violation of the rules	A warning or a fine of GEL 2,000						A warning or a fine of GEL 4,000		
Transfer in violation of the rules (in the presence of aggravating circumstance(s))	Fine GEL 4,000						Fine GEL 6,000		

Sanctions

	Natural person	State authority	N(N)LE	Legal person	Branch	I/E	Legal person	Branch	I/E
				Annual turnover < GEL 500,000			Annual turnover > GEL 500,000		
Violation of the rules for submitting information and/or documents to the head of the Personal Data Protection Service or an authorized person or providing false information									
Violation of the rules for submitting information and/or documents or providing false information	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		
The same action committed by a person who was subject to an administrative fine within 1 year	Fine GEL 3,000						Fine GEL 5,000		
Obstructing the head of the Personal Data Protection Service or the authorized person to exercise the right provided for by the law									
Obstructing the exercise of the right by the authorized person	A warning or a fine of GEL 2,000						A warning or a fine of GEL 4,000		
The same action committed by a person who was subject to an administrative fine within 1 year	Fine GEL 4,000						Fine GEL 6,000		
Failure to comply with the legal requirements of the Personal Data Protection Service	A warning or a fine of GEL 1,000						A warning or a fine of GEL 2,000		

Failure to fulfill the obligation regarding the appointment of the personal data protection officer	Warning
Failure to fulfill the obligation regarding the appointment of the personal data protection officer within 1 year from the imposition of an administrative fine	Fine GEL 3,000
Failure to fulfill the obligation related to the designation/appointment of a special representative	A warning or a fine of GEL 3,000
Failure to fulfill the obligation related to the designation/appointment of a special representative within 1 year from the imposition of an administrative fine	Fine GEL 5,000

Roadmap

Contact us

Giorgi Lomidze
Manager

KPMG Law Georgia
Tel.: +995 599 306080
Email: glomidze@kpmg.com

Mariam Chakvetadze
Senior lawyer

KPMG Law Georgia
Tel.: +995 593 304130
Email: mchakvetadze@kpmg.com