DATA PROTECTION LAWS OF THE WORLD

Georgia

GEORGIA

Last modified 22 December 2021

LAW

The Law of Georgia On Personal Data Protection (N5669-RS, 28/12/2011) (‘**PDP Law**’).

DEFINITIONS

Definition of Personal Data

Personal data: any information connected to an identified or identifiable natural person. A person is identifiable when he/she may be identified directly or indirectly, in particular by an identification number or by any physical, physiological, psychological, economic, cultural, or social features specific to this person.

Definition of Sensitive Personal Data

Special category data: data connected to a person's racial or ethnic origin, political views, religious or philosophical beliefs, membership of professional organisations, state of health, sexual life, criminal history, administrative detention, putting a person under restraint, plea bargains, abatement, recognition as a victim of crime or as a person affected, also biometric and genetic data that allow to identify a natural person by the above features.

Biometric data: Any physical, mental, or behavioural feature which is unique and constant for each natural person and which can be used to identify this person (fingerprints, footprints, iris, retina (retinal image), facial features).

Genetic data: Unique and constant data of a data subject relating to genetic inheritance and/or DNA code that makes it possible to identify them.

NATIONAL DATA PROTECTION AUTHORITY

State Inspector Service (‘State Inspector’).
www.personaldata.ge

REGISTRATION

With certain exceptions (discussed below), there is no requirement under PDP Law to notify or register before processing personal data.

The registration requirement applies to the databases. According to the PDP Law, a database is any structured set of personal data where data is arranged and can be accessed based on certain criteria. The PDP Law uses the term filing system to denote a database. For example, a customer database or a registry of employees and clients that is subject to processing may qualify as a filing system.

The data controller is obliged to have a catalogue on each filing system that provides a detailed description of the filing system's structure and content.

According to the PDP Law, before creating a filing system and entering in any new category of data, a data controller shall notify the State Inspector and register the following information about the filing system:

- The name;
- The names and addresses of a data controller and a data processor;
- The place of storing or processing of data;
- The legal grounds for data processing;
- The category or categories of data subjects;
- The data category or categories in a filing system;
- The purpose of data processing;
- The period of data storage;
- The facts and grounds for restriction (if any) of any data subject rights;
- The recipient of data stored in a filing system, and their categories;
- Information on any cross-border data transfer and transmission of data to international organisation and the legal grounds for the transfer;
- A general description of the procedure established to ensure data safety.

The data controller shall regularly update the filing system catalogue and notify the Inspector about any alteration made to the information, no later than 30 days after the alteration.

The notification requirement also applies to cross-border data transfer and a private organisation's processing of a biometric data.

Before using the biometric data, a data controller must provide the State Inspector with the same information that is provided to the data subject, specifically the purpose of data processing and the security measures taken to protect the data.

DATA PROTECTION OFFICERS

None.

COLLECTION & PROCESSING

The following minimum requirements must be met when collecting or otherwise processing the personal data:

- A proper legal ground (for example, a data subject's consent) exists to process the data;
- The personal data is processed for specific, clearly defined, and legitimate purposes;
- The personal data is processed only to the extent necessary for legitimate purposes;
- The personal data is adequate and proportionate to the purpose or purposes for which it was collected and processed;
- The data is kept only for the period necessary to achieve the processing's purpose;
- The data controller or data processor takes technical and organisational security measures to ensure the protection of personal data against accidental or illegal destruction, modification, disclosure, access, and any other form of illegal use or accidental or illegal loss;
- The security measures implemented are appropriate to the risks related to the data processing.

TRANSFER

Transfer of personal data outside Georgia is admissible without a separate authorisation from the State Inspector if one of the two following conditions apply:

- A respective legal ground for data processing exists and the proper standards for the safety of data are secured in the relevant country. The State Inspector has approved the list of such countries;
- The processing of data is stipulated under an international agreement between Georgia and the relevant country;

However, the general data processing rules will still apply, including securing a necessary legal ground such as the data subject's consent and the requirements of proportionality and necessity.

If neither of these conditions apply, then there should be a formal written agreement between the transferor and the data's recipient under which the data's recipient shall commit to ensure proper guarantees to protect the data. In this case, the State Inspector must be presented with such agreement and other relevant information or documents for data transfer approval.

SECURITY

A data processor must implement technical and organisational security measures to ensure the protection of personal data against accidental or illegal destruction, modification, disclosure, access, and any other form of illegal use or accidental or illegal loss. The security measures implemented must be appropriate to the risks related to the data processing.

A record must be kept of all data processing activities carried out on personal data stored in electronic form. A record must also be kept of any disclosure or modification of personal data contained in non-electronic form.

Employees of a data controller or a data processor who are involved in data processing must not act beyond the scope of the powers conferred upon them. Employees must be bound to protect confidentiality of the personal data, including after termination of their official duties.

BREACH NOTIFICATION

None.

ENFORCEMENT

The State Inspector has power to carry out inspections of any data controller and data processor on its own initiative or based on complaints received from data subjects.

The State Inspector may order:

- Temporary or permanent termination of data processing;
- The blocking, destruction, or depersonalisation of personal data;
- The termination of transfer;
- An issuance of administrative fines.

The State Inspector also has a duty to report any violations of a criminal nature to the competent authority. The liability for violation of the data privacy can be criminal, administrative or civil.

Criminal liability: a fine, correction labour, imprisonment for three years, or all three may result from illegal collection, retention, use, or dissemination of personal data that caused substantial damage; A legal entity may be imposed a fine, deprivation of the right to run the business, liquidation and a fine for the same action.

Administrative sanctions: ranging from GEL500 (app. USD 160) to GEL10,000 (app. USD 3200) depending on the type of violation.

Civil: claims can be brought by individuals, depending on the damage the breach of the PDP Law caused.

ELECTRONIC MARKETING

PDP Law defines direct marketing as offering of goods, services, employment, or temporary work by mail, telephone calls, email, or any other telecommunication facility.

Consent is not required to process personal data obtained from public sources for direct marketing purposes. The data permissible to be collected from publicly available sources is limited to: name and surname, telephone number, email, and fax number.

However, written consent is required if the data processor wishes to use other types of personal data for direct marketing purposes.

Individuals are entitled to demand the termination of using their data for direct marketing purposes at any time in the form under which the direct marketing is conducted.

ONLINE PRIVACY

There is no special regulation with respect to cookies and general rules on data collection and processing applies. Georgian web-sites routinely ask for cookie consent.

There is no requirement to store data in Georgia. However, rules on cross border data transfer will apply.

KEY CONTACTS

MKD Law
mkdlaw.ge/en

Baqar Palavandishvili
Lawyer
MKD Law
T +995 32 2553880/81
bpalavandishvili@mkdlaw.ge

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.