Data Protection in Georgia

KAGENCY

SUMMARY

OVERVIEW

Georgia adopted the Data Protection Act on 28 December 2011, which serves as the fundamental legal framework for data processing and protection activities in Georgia. The Data Protection Act reflects Georgia's commitment to the 2005 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Several legal acts contribute to the data protection framework in Georgia. Additionally, the Data Protection Act was impacted by the Data Protection Directive (GDPR). The report on data protection in Georgia will offer a comprehensive overview of the data protection framework in Georgia, the mechanisms used, and the impact of the General Data Protection Directive (GDPR) on Georgian data protection legislation and Georgian business activities in Europe.

GOVERNING TEXTS

Georgia's legislation governing personal data protection has developed significantly over the past decade.

Currently, the primary Law governing data protection in Georgia is the Data Protection Act adopted on 28 December 2011. Other normative acts regulating data protection in Georgia are:

- Law of Georgia on State Inspector Service from 21.07.2018
- Resolution of the Government of Georgia on the Approval of the Regulations on the Activities of the Personal Data Protection Inspector and the Rule of Exercising the Power by Him/Her

In May 2019, the Office of the Personal Data Protection Inspector (“PDP”) registered with the Parliament of Georgia the draft law On Personal Data Protection (“The Draft Law”), though it hasn’t entered into force yet. The Draft Law's objective is to incorporate comprehensive data protection regulations into Georgian Law and ensure compliance with the General Data Protection Regulation (GDPR).

The adoption of the new legislation will significantly increase the quality of personal data protection in Georgia, bringing the country even closer to the EU standards and creating an opportunity for Georgia to become a leading country in the Caucasus region in the field of data protection.

Although General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR) governs data protection in the European Union, it had a significant impact on Georgia as well, as GDPR applies both to legal entities based on the territory of the European Union and to

companies that provide products or services to entities located on the EU territory or monitor the behaviour of natural persons.

The current Georgian legislation on data protection applies to the processing of data of Georgian citizens. Therefore, GDPR extends its authority toward Georgian companies that perform the processing of EU citizen data.

Since GDPR entered into force, the interest of the Georgian companies doing business with Europe has increased significantly towards the European legislation, particularly in the areas of the extension of GDPR to the activities of Georgian-based companies, the obligation to appoint a representative in the European Union, the exchange of information with the companies based on the territory of the European Union, among many.

SCOPE OF APPLICATION

The Data Protection Act applies to:

- processing personal data through automatic or semi-automatic means on the territory of Georgia;
- processing data through non-automatic means within the territory of Georgia, which data forms part of the filing system or are intended to form part of the filing system; and
- automatic processing of data defined as a state secret for the purposes of crime prevention and investigation, operational-investigative activities and protection of the rule of Law.

Processing personal data on Georgian territory will trigger the application of the Data Protection Act. If this is the case, the data controller's nationality or residence is irrelevant. The territoriality of the data processing activity is the deciding factor.

The Data Protection Act does not apply in case data processing is conducted by a natural person for personal purposes not related to his professional or entrepreneurial activities. It also does not apply during court proceedings if the data may prejudice the outcome before the decision on the case is made and in case of state secret protecting state security, defence, intelligence, or counterintelligence.

The requirements that data controllers maintain a file system catalogue and notify and register certain information with the State Inspector do not apply to political parties, professional and other unions, and religious groups processing data about their members. Also, special category data processing rules do not apply to data processing used for public safety, criminal investigations, and operational and investigative activities.

DATA PROTECTION AUTHORITY & REGULATORY AUTHORITY

The State Inspector Service is tasked with aligning Georgian data protection legislation with the European standards, which is the prerequisite of the Association Agreement between the European Union and Georgia.

The Office of the State Inspector is the data protection regulator. The State Inspector Office has succeeded the Office of the Personal Data Protection Inspector.

The State Inspector has three primary responsibilities:

- controlling the legality of data processing activities;
- monitoring of secret investigative actions and activities carried out in the central bank of electronic communication identification data; and
- investigation of crimes committed by the representatives of the law enforcement institutions, officers, or persons equal to them.

The State Inspector also inspects data processing activities in public and private organisations, provides data protection consulting to public and private entities, examines data subject applications, and maintains a registry of filing system catalogues.

In 2021, a group of non-governmental organisations conducted a study on the efficiency of the work of the State Inspector, providing a range of recommendations to the Georgian Parliament. The report, covering activities of FY2020, was submitted in April 2021. Nevertheless, the Parliament has not considered the report yet. The review period has been extended three times so far.

Throughout 2021, to improve data protection standards, the State Inspector Service was tasked with raising public awareness about data protection and implementing prevention-oriented policies. Large-scale projects covered all parts of the country with activities such as hosting student forums and conferences, school competitions, meetings between local governments and civil sectors, publication of the thematic report by the State Inspector Service, coordinated training for public and private sector representatives, and development of the tools to measure personal data protection in Georgia. The State Inspector Service actively monitors data processing in public and private sectors with a focus on large data processing organisations.

Nevertheless, Georgia's focus on adherence to the fundamental data protection principles remains challenging. In 2021, thousands of files which contained information on private communications of the clergy of the high hierarchy of the Patriarchate were leaked, spreading

across social networks and the media. The leaked documents caused another public scandal in Georgia as the files were assumed to be obtained in secret surveillance by the State Security Service.

On December 29, 2021, the Georgian Parliament adopted the Bill on State Inspector Service in the first reading, which divides the State Inspector Service into two agencies — Special Investigation Service and Personal Data Protection Service. The Special Investigation Service will investigate the official misconduct, and the second agency will ensure the control of legality of the data processing activities and monitor the covert investigation and e-communication identification in the Central Data Bank.

KEY DEFINITIONS

Data controller is a public authority or natural or legal person who, individually or in cooperation with others, determines the purposes and means of personal data processing and processes the personal data directly or via a data processor.

Data processor is any natural or legal person processing the personal data for or on behalf of the data controller.

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

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

Biometric data is 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).

Pseudonymisation is data depersonalisation is defined as data modification in a way to make it impossible to link the data to the data subject or to require disproportionately great effort, expense and time to establish such a link.

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

PRINCIPLES

Data controllers may process personal data in the form and manner permitted by the Law, including:

- processing personal and special category data;
- processing the data for direct marketing purposes; and
- conducting video surveillance.

Data controller's primary responsibility is to ensure that the following requirements are met:

- there is a proper legal ground to process personal data, such as the data subject's consent;
- personal data is processed for specific, clearly defined, and legitimate purposes;
- personal data is processed only to the extent necessary for legitimate purposes;
- personal data is adequate and proportionate to the purposes for which it was collected;
- the data is kept only for the time period necessary to achieve the defined purpose of data processing;

- the data controller and data processor took necessary security measures to ensure the protection of personal data from accidental or illegal destruction, modification, disclosure, access, and any other form of illegal use or accidental or illegal loss; and
- the security measures implemented by the data controller and data processor are adequate for the risks of personal data processing.

CONTROLLER AND PROCESSOR OBLIGATIONS

The necessity for registration (notice) also applies to databases. A database, as defined in Article 2(N) of the Data Protection Act, is any structured collection of personal data that is organised and searchable according to specific criteria. The Data Protection Act uses the phrase filing system to refer to a database. For instance, a customer database or a processed registration of employees and clients may qualify as a filing system.

According to Article 19 of the Georgian Data Protection Act, the data controller is required to maintain a separate catalogue for each filing system that contains a full description of the filing system's structure and content. Prior to the establishment of a filing system and the electronic input of a new category of data, the data controller must register with the State Inspectorthe following information:

- the name of the filing system;
- names and addresses of a data controller and a data processor, place of storing, and/or processing of data;

- legal grounds for data processing;
- the category of the data subject;
- the category of data in the filing system;
- the purposes of data processing;
- the period for data storage;
- the fact and grounds for the restriction of a right of a data subject;
- the recipient of data stored in a filing system and their categories;
- the information on the trans-border flows of data and transmission of data to an international organisation, and the legal grounds for the transfer; and
- the general description of the procedure established to ensure data security.

Data controllers are responsible for maintaining an up-to-date file system catalogue. Any modification to the information contained in the file system catalogue must be reported to the State Inspector within 30 days of the modification.

Notification is also required for cross-border data transfers and private companies' handling of biometric data.

Before using biometric data, a data controller must provide the same information as is supplied to the data subject to the Inspector, specifically the purpose of data processing and the security measures in place to secure the data subject's personal information.

Transfer of personal data outside of Georgia is admissible without a separate authorisation from the State Inspector in case either the relevant country has established a respective legal ground for data processing, proper standards for data safety are secured, or the data processing is stipulated in the international agreement between Georgia and the relevant country. If neither of the conditions applies, a formal written agreement should be entered into between the transferor and the receiver, in which the recipient commits to providing adequate safeguards to preserve the data. In this situation, the State Inspector must be supplied with the agreement and any other pertinent information or documents to obtain clearance for the data transfer.

The data processor is required to maintain records of all data processing actions performed on personal data that is stored electronically. Additionally, any disclosure or alteration of non-electronic personal data must be documented.

Currently, the Data Protection Act makes no provision for an obligation to make a Data Protection Impact Assessment/Privacy Impact Assessment. Appointing a data protection officer is not a mandatory necessity. There is no direct obligation to notify a data breach to the State Inspector.

The Data Protection Act makes no provision for the duration of data storage. The data controller chooses the duration of data retention on his or her own.

Following the general principle of the Data Protection Act, personal data may only be retained as long as it is necessary to achieve the legitimate objectives for which the data was collected. After such purposes have been achieved, personal data must be blocked, deleted, destroyed, or retained in a form that prevents the identification of an individual unless otherwise provided for by the Data Protection Act.

As confirmed by State Inspector rulings, it is not legal to store data indefinitely.

Article 71 of the Child's Code of Rights prohibits the disclosure of personal data about a child involved in administrative or judicial proceedings in any form, including through media, that could reveal or indirectly indicate the child's identity (an image, a detailed description of the child or his/her family members, names, addresses, audio and video recordings, and similar information).

Additionally, it is prohibited to disclose in any form, including through the media, a document or record containing personal data about a child that is related to the use of disciplinary measures against the child, violence committed against or by the child, the child's health status, the child's participation in social assistance or charity programs for disabled children or poor families, or other similar information.

The processing of special category data is prohibited by law except with the written consent of the data subject or in case one of the following conditions apply:

- the data subject has made public the data about him/her, without expressly prohibiting the use of such data;
- processing of health-related or prior conviction data is necessary for the data controller to observe the employment obligation, including for hiring the candidate;
- data processing is necessary to protect the vital interests of the data subject or a third party, and the data subject is physically or legally disabled to provide consent for data processing;
- the data are processed to protect the public health, processed by a healthcare facility (employee of such facility) for the purpose of protecting an individual's health, or processed where necessary for the management or operation of the healthcare system;
- data processing is carried out by political, philosophical, religious, or trade unity, association, or other non-commercial organisation while performing legitimate activities. If this is the case, data processing may only be related to the members of such organisation or to the persons who have a permanent connection with the organisation;
- data is processed to run the registry/personal files of the accused/convicted individuals; to consider the issues related to individual planning of serving a sentence by the convicted person and/or releasing a convicted person on parole and changing of an unserved term with a lighter punishment; and
- data are processed under Law of Georgia On Crime Prevention, Non-Custodial Sentences, and Probation (only available in Georgian here), Law of Georgia On International Protection (only available in Georgian here), or for the functionality of a uniform analytical system of migration data.

When processing special category data is based on any of the grounds above, it is prohibited to publish or disclose the data to third parties without the data subject's consent.

A data processor may carry out data processing based on legal action, or a written agreement with the data controller. The agreement must meet the requirements of the Data Protection Act and other legal acts and include the prohibitions set out in the Data Protection Act.

DATA SUBJECT RIGHTS

Right to be informed: When personal data is collected directly from a data subject, the data controller or data processor must provide the data subject with the following information:

- identities and registered addresses of the data controller and the data processor (if applicable);
- purposes of the data processing;
- whether the provision of data is mandatory or voluntary and, if mandatory, the legal consequences of refusal to submit them; and
- the right of the data subject to obtain information on their personal data processed, request their correction, updating, addition, blocking, deletion, and destruction.

Provision of the information is not mandatory if the data subject already has it.

Right to access: The data subject has the right to request information from a data controller on the processing of their data. Upon request, the data controller must provide the data subject with the following information:

- which personal data was processed;
- the purpose of data processing;
- the legal grounds for data processing;
- the ways in which the data were collected; and
- to whom the personal data were disclosed, and the grounds and purpose of the disclosure.

The data subject must be supplied with the information outlined above immediately upon request or not later than ten days after the request is made. When responding to the request, it is required to:

- retrieve and process the information at another institution or structural unit or consult with either one;
- retrieve and process voluminous documents not linked to each other; and
- consult with its structural unit located in another populated place or with another public agency.

Right to rectification: Upon the data subject's request, the data controller must correct, update,

add, block, delete, or destroy the personal data if it is incomplete, inaccurate, outdated or collected in violation of the Data Protection Act.

Right to erasure: Upon request of the data subject, the data controller must delete or destroy the personal data if they are incomplete, inaccurate, outdated, or collected in violation of the Data Protection Act.

Ri*ght to object/opt-out:* A data subject may revoke consent on data processing and request termination of data processing or deletion of processed data at any time and without explanation. This data subject's right does not apply to the data processed with consent and is related to the performance of a monetary obligation.

Right not to be subject to automated decision-making: The Data Protection Act does not provide any specific provision on data subjects' right not to be subject to automated decision-making.

Right to appeal: The data subject may appeal the violation of their rights before the State Inspector, the Court, or the administrative body.

PENALTIES

A breach of the Data Protection Act may result in criminal, administrative, and civil liability.
Criminal liability: The unauthorised collection, retention, use, or dissemination of personal data that results in severe damage is punishable by a fine, correction labor, and/or three years in prison. The legal entity may be fined, denied the right to conduct business, or forced into liquidation and fined.

Administrative sanctions: The State Inspector has the authority to order the suspension or termination of data processing, the blockage, destruction, or depersonalisation of personal data, the cessation of transfer, and the imposition of administrative fines.

The administrative fines set out under the Data Protection Act range from GEL 500 (approx. €125) to GEL 10,000 (approx. €2,500), depending on the type of violation.

Civil claim: Individuals may also bring a civil claim depending on the harm caused by the breach of the Data Protection Act.

Georgia's Supreme Court has rendered several important enforcement rulings. One of them concerns the processing of deceased individuals' personal data. The Supreme Court cited article 7.5 of the Data Protection Act, which allows for disclosing a deceased person's data for historical, statistical, and research purposes. The only exception applied in the case when the deceased person expressly banned dissemination of their data in writing, and the court determined that this is an acceptable legislative basis for processing the deceased's personal data. The Supreme Court stated, however, that the person seeking access to the deceased person's data on that basis must establish a statutory basis and compelling public interest for such access.

CONCLUSION

Being in the process of European integration, Georgia needs to adapt its legislation to the European standards fully. Effective steps to establish a high standard of personal data protection must continue. The introduction of European standards for personal data protection will be a step forward for Georgia to integrate into the European single digital market. Georgian citizens will benefit from higher security standards and effective and efficient human rights protection mechanisms, including the right to privacy in processing personal data.

To achieve these goals, Georgia needs to focus on:

- Creating organised and effective legislation on data protection;
- Establishing a clear definition of competency of cyber security authority with the State Inspector's office on issues related to personal data processing, including authority in the event of data breach and/or cyber incident;
- Establishing a protocol for mutual exchange of information and legal procedural norms by the State Inspector's office and cyber protection authority;
- Establishing clear criteria for identifying subjects of critical information systems and requirements for the development of internal data protection policy documents (bylaws);
- Aligning responsibility for a data breach following the GDPR standards;
- Increasing responsibility of data protection for public and private sectors
- Continuing raising awareness and conducting training on data protection among private and public sectors.

SOURCES

- Georgia - Data Protection Overview 2022
- Data Protection Report 2018
- Data Protection Report 2017
- Law of Georgia on Personal Data Protection
- Two Years Since the Enforcement GDPR And Its Impact On Georgia
- რა ხარვეზებს შეიცავს სახელმწიფო ინსპექტორის სამსახურთან დაკავშირებული საკანონმდებლო პაკეტი / What are the shortcomings of the legislative package related to the state inspector's service?
- მედიით ვრცელდება, თითქოს, სუს-ის მიერ სასულიერო პირებზე ფარული მიყურადების მემცველი ჩანაწერები / Records allegedly containing secret surveillance of clerics by SUS are circulating in the media, Radio Tavisupleba
- კიბერსივრცეში პერსონალური მონაცემების დაცულობის უზრუნველყოფა: გამოწვევები და საჭიროებები საქართველოსთვის / Ensuring security of personal data in cyberspace: challenges and needs for Georgia, Institute for Development of Freedom of Information
- Data Protection Law in Georgia, DLA Piper

347 Fifth Ave, Suite 1402
New York, NY
10016

+1 (413) 645-4564
hello@bkagency.co
www.bkagency.co