EVALUATION OF PLANNED AMENDMENTS TO THE LAW ON PERSONAL DATA PROTECTION

TRANSPARENCY INTERNATIONAL GEORGIA

Parliament of Georgia registered a legislative initiative submitted by MPs whose goal is to align the legislation regulating personal data protection with the laws of the European Union and to fulfil the obligations under the Association Agenda.

The legislative proposal made by the Staff of the Personal Data Protection Inspector served as the basis for the legislative initiative.

DRAFT LAW AND ITS INITIATOR

Legislative initiative: Draft amendments to the Law on Personal Data Protection and related laws.

Initiators: Sopio Kiladze, Rati Ionatamishvili, Tsotne Zurabiani, Vano Zardiashvili, Irakli Beraia, Anri Okhanashvili

Author: Service of State Inspector

ESSENCE OF THE DRAFT LAW

According to the explanatory note, the main purpose of the legal amendments is to align the legislation with the regulations of the EU.

On 25 May 2018, the new regulation to protect personal data – General Data Protection Regulation (GDPR) was put into effect on the territory of the EU, which considerably improved the standards of personal data protection. This regulation applies to all organisations registered in the EU as well as organisations that supply services or goods to the citizens of the EU.

In turn, according to Annex I of the Association Agreement, Georgia is under the obligation to ensure the alignment of the personal data protection legislation with the EU Directive No 95/46/EC. This directive was replaced with GDPR in 2018.

The draft contains the following main amendments:

- Processing data in the absence of consent with the aim of direct marketing will be restricted despite their public availability;
- The "right to be forgotten" will be realised, including a person's right to demand the erasure of links to his or her personal data;
- There will be fewer grounds for data processing;
- Rules of processing underage persons' data will be made more specific;
- An institute of Personal Data Protection Officer will be created in public institutions and large organisations;
- An obligation to report incidents to the Service of State Inspector will be introduced and so on.

1. CONSENT TO THE PROCESSING OF INFORMATION WITH THE PURPOSE OF DIRECT MARKETING

CURRENT REGULATION	PROPOSED AMENDMENT
Processing data for the purpose of direct marketing does not require consent from the data subject if the information is available from public sources.	Processing data for the purpose of direct marketing will be allowed only with the consent of the data subject. The data processor/authorised person, prior to receiving consent from the data subject and during the implementation of direct marketing, will have an obligation to explain to the data subject *clearly and in simple language* his/her right to withdraw his/her consent at any time and the mechanism/rule of exercising this right.

2. RIGHT TO STOP DATA PROCESSING, ERASE OR DESTROY DATA (RIGHT TO BE FORGOTTEN)

CURRENT REGULATION	PROPOSED AMENDMENT
If requested, the data processor is obliged to correct, update, add, block, erase or destroy data if they are incomplete, inaccurate, outdated or if their collection and processing was done in violation of the law.	The data subject has the right to demand to stop processing data about him/her, erase or destroy them if: • The data processing is no longer necessary for the purpose for which they were processed; • The data subject withdraws consent which constitutes the only basis for data processing; • The data processing took place / is taking place in violation of the law. The data subject also has the right to demand from any data processor to erase all links to their data.

3. SANCTIONS FOR VIOLATING THE RULES OF DIRECT MARKETING

CURRENT REGULATION	PROPOSED AMENDMENT
• GEL 3,000 fine; • Fine for repeat violation – GEL 10,000.	• GEL 2,000 fine if the turnover of physical or legal person does not exceed GEL 50,000; • Fine for repeat violation – GEL 4,000; • GEL 3,000 fine if the turnover of a legal person (except for N(N)LPs) exceeds GEL 50,000; • Fine for repeat violation – GEL 6,000.

4. GROUNDS FOR DATA PROCESSING

CURRENT REGULATION	PROPOSED AMENDMENT
• Existence of data subject's consent; • If it is required for the data processor to fulfil obligations envisaged by the law; • If it is required to protect vital interests of the data subject; • If it is required to protect legal interests of the data processor or a third party; • Data processing is envisaged by the law; • Data processing is necessary to protect an important public interest in accordance with the law; • In accordance with the law, the data are publicly available or the data subject made them available; • Data processing is necessary to consider the application submitted by the data subject (in order to provide him/her with a service).	• Data subject gave his/her consent; • If it is required to fulfil an agreement made with the data subject or to make a deal requested by the data subject; • If it is required to protect vital interests of the data subject or other person; • If it is required for the data processor to fulfil the obligations envisaged by the law; • If it is required to fulfil the tasks within the area of public interest (crime prevention, investigation and others); • If it is necessary to protect legal interests of the data processor or a third party.

5. PERSONAL DATA PROTECTION OFFICER

CURRENT REGULATION	PROPOSED AMENDMENT
No such institution exists	The listed organisations will have an obligation to appoint or allocate a Personal Data Protection Officer to ensure provision of information about data processing: • Public institutions; • Insurance companies; • Commercial banks; • Micro-finance organisations/credit bureaus; • Electronic communications companies; • Airlines; • Airports; • Medical institutions which provide services to at least 10,000 data subjects per year; • Data processor which processes data for a large number of data subjects or implements a systemic and large-scale monitoring of their behaviour.

6. PROCESSING UNDERAGE PERSONS' DATA

CURRENT REGULATION	PROPOSED AMENDMENT
No special regulation for underage persons exists	Processing of underage person's data is permitted on the basis of his/her consent if he/she has reached the age of 14 years old, while those of underage person younger than 14 – based on the consent from his/her parents or other legal representative.[1]

7. OBLIGATION TO REPORT INCIDENTS TO SERVICE OF STATE INSPECTOR

CURRENT REGULATION	PROPOSED AMENDMENT
No such obligation exists	Data processor/authorised person is under the obligation to record an incident, its result, measures carried out and, no later than within 72 hours from the discovery of the incident, report it to the Service of State Inspector.[2]

8. LIST OF PERSONAL DATA IDENTIFIERS

CURRENT REGULATION	PROPOSED AMENDMENT
A person is identifiable when it is possible to identify him/her directly or indirectly: • By identification number; • By a physical, physiological, psychological, economic, cultural or social feature.	A person is identifiable when it is possible to identify him/her directly or indirectly: • By name, last name; • By identification number; • By geolocation data; • By identifiable data of electronic communication; • By a physical, physiological, mental, psychological, genetic, economic, cultural or social feature.

EVALUATION/RECOMMENDATIONS

Aligning personal data protection regulations with the legislation of the EU and fulfilment of the obligations under the Association Agenda deserve a positive evaluation.

It is important for the EU regulations to be reflected exactly in the legislation and to be implemented within a reasonable timeframe. The grounds for information processing envisaged by the draft law are not fully compliant with the standards set by GDPR and are vague. GDPR provides for the authority of the state to establish certain exceptions based on public and legitimate interests, which should receive appropriate consideration during the process of elaboration of this legislation.

The draft law contains several problematic issues:

- The draft law envisages restricting the grounds for data processing, which means that it would also be impossible to process data which, according to the law, are already public and available to everyone. This amendment significantly changes the balance against transparency and openness. The draft law does not allow processing such information even when the goal of such processing is the provision of such public goods as, for example, combating corruption, transparency of public finances and so on.
- The draft law does not reflect the decision made by the Constitutional Court on 7 June 2019 which deemed unconstitutional the normative content of Articles 5 and 6 of the current law which prohibited requesting court rulings as public information. This court decision will come into force on 1 May 2020, and passing this draft law without considering it will create the need to amend it before May of next year.
- The amendments envisaged by the draft law and the most significant ones throughout the existence of this law, it creates essentially new obligations for all data processors throughout the country. The draft law indicates a six-month term for being put into effect; GDPR itself was adopted in 2016 and put into effect two years later, in 2018. A large-scale information campaign is necessary although even in this case it will be difficult to inform all parties about the new legal requirements in such a short period of time so that no *en masse* violation of the law takes place.

Recommendations

- The grounds for data processing must clearly envisage a possibility for such processing of already public data which would serve public and legitimate purpose;
- The draft law must consider the standard of openness with regard to court rulings established by the Constitutional Court decision of 7 June 2019;
- The term for putting the law into effect must be deferred for more than six months;
- The Staff of the State Inspector must use the remaining time as efficiently as possible to familiarise the target parties with the new requirements of the law.

1 GDPR sets the age of consent at 16 years old but allows member states to determine this age themselves provided it is not younger than 13 years old.

2 Incident – actual violation of data security or potential threat of such violation, which is carried out using information technologies and causes or could cause the data to be made public without permission, damaged, destroyed, lost, changed, be accessed without authorisation, collected/obtained, and which violates or threatens the rights and/or interests of the data subject.

Norwegian Ministry of Foreign Affairs

The publication was prepared with the financial support of the Norwegian Ministry of Foreign Affairs.