DATA PROTECTION LAWS OF THE WORLD

Uzbekistan

DLA PIPER

UZBEKISTAN

Last modified 22 January 2024

LAW

Until recently, Uzbekistan did not have a stand-alone personal data protection law. The situation changed with the adoption on 2 July 2019 of the Law of the Republic of Uzbekistan No. ZRU-547 “On Personal Data” (“**Law on Personal Data**”), which entered into force on 1 October 2019.

With the entry into force of the Law on Personal Data, a unified set of main rules and requirements in the area of data protection and processing that is aimed at substantial regulation of these issues was introduced in Uzbekistan.

The scope of application of this Law is rather broad, as it applies to *relations arising from processing and protection of personal data, regardless of the applied means of processing, including information technologies*.

Apart from the Law on Personal Data, there are certain legal acts that establish fundamental principles of data protection processing and / or set liability for violation of data protection rules. They include:

- Constitution of the Republic of Uzbekistan (in the new edition), effective from 1 May 2023;
- Civil Code of the Republic of Uzbekistan, effective from1 March 1997;
- Labour Code of the Republic of Uzbekistan (in the new edition), effective from 30 April 2023;
- Code of the Republic of Uzbekistan on Administrative Liability, effective from 1 April 1995 (‘Code on Administrative Liability’);
- Criminal Code of the Republic of Uzbekistan, effective from 1 April 1995 (‘Criminal Code’);
- Law No. 439-II 'On Principles and Guarantees of Freedom of Information' dated December 12, 2002; and
- Law No. 560-II 'On Informatization' dated December 11, 2003.

Lastly, there are also sector-specific laws applicable depending on the type of industry. Data protection regulation exists mainly in financial, telecommunication, health and insurance sectors and consists of the following legal acts:

- Law No. 530-II 'On Bank Secrecy' dated August 30, 2003, under which a bank is prohibited to disclose bank secrecy, and should guarantee its protection;
- Law No. 822-I 'On Telecommunications' dated August 20, 1999, under which all operators and service providers are obliged to ensure the secrecy of communications;
- Law No. 265-I 'On Protection of Citizens’ Health' dated August 29, 1996, under which the medical secrecy is protected; and
- Law No. ZRU-730 'On Insurance Activities' (in the new edition) dated November 23, 2021, under which insurance companies should guarantee the confidentiality of information which became available in course of provision of insurance services.

DEFINITIONS

Definition of personal data

The Law on Personal Data defines **Personal Data** as information recorded on electronic, paper and / or other tangible medium, relating to a specific individual or that allows to identify such individual (i.e. ‘**subject of personal data**’).

Apart from the above, the Law on Personal Data distinguishes separate types of personal data in respect of which the Law imposes a special processing and protection regime. They include:

- **special personal data**, i.e. data about racial or social origin, political, religious or ideological beliefs, membership in political parties and trade unions, as well as data regarding physical or mental health, information about private life and criminal records;
- **biometric personal data**, i.e. personal data characterizing anatomical and physiological characteristics of the subject of personal data; and
- **genetic personal data**, i.e. personal data related to the inherited or acquired characteristics of the subject of personal data, which is the result of the analysis of the biological sample of the subject or the analysis of another element that allows to obtain equivalent information.

Definition of sensitive personal data

The Law on Personal Data does not provide for an express definition of sensitive personal data. Yet, it distinguishes the category of *special personal data*. Under the foregoing Law, special personal data includes:

- data about racial or social origin;
- data about political, religious or ideological beliefs;
- data about membership in political parties and trade unions;
- data about physical and mental health; and
- data about private life and criminal records.

NATIONAL DATA PROTECTION AUTHORITY

The Law on Personal Data designates the Cabinet of Ministers of the Republic of Uzbekistan (the '**Cabinet of Ministers**') and State Personalization Centre under the Cabinet of Ministers (the ‘**State Personalization Centre**’) as the main regulatory authorities in respect of the protection of personal data. That said, following the recent administrative reform, the State Personalization Centre was reorganised into the Personalization Agency under the Ministry of Justice of the Republic of Uzbekistan (the '**Personalization Agency**’).

Additionally, following the latest amendments to Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 707 “On Measures for Further Improvement of Information Security in Internet” dated September 5, 2018 (“ **Resolution No. 707**”) adopted in pursuance of the recently introduced localization requirement, the State Inspection of the Republic of Uzbekistan on Informatization and Telecommunication was designated as a state authority empowered, *inter alia*, to:

- implement the state control over the activity of personal database owners and operators by monitoring their activities;
- issue notifications, instructions, as well as orders that are to be fulfilled by public authorities, individuals and / or legal entities, in order to ensure compliance with the data protection laws;
- maintain the Register of Infringers of the Rights of Personal Data Subjects.

REGISTRATION

The Law on Personal Data requires a personal data database to be registered with the State Registry of Personal Databases maintained by the Personalization Agency. The registration should represent a simple notification with the Personalization Agency.

The registration is performed by an owner / operator of personal database by way of notification, i.e. by approaching the Personalization Agency in person or via its website (Government registry for personal databases).

The registration procedure for personal database is mainly set forth by the Regulation on the State Register of Personal Databases, approved by the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 71 dated February 8, 2020 (‘**Regulation No. 71**’).

Under Regulation No. 71, to register a personal database, an owner / operator of personal data is required to fill and submit the application as per the prescribed form to the Personalization Agency. In its turn, the Personalization Agency shall review the submitted application within 15 days from the date of its receipt. Based on the results of such review, the Personalization Agency either agrees or refuses to register the database. In case of a positive decision, the Personalization Agency issues a certificate on registration of a personal database to an owner / operator of personal data.

The registration is not required for databases containing personal data:

- relating to participants / members of a public association or religious organization and processed accordingly by a public association or religious organization, provided that personal data will not be distributed or disclosed to third parties;
- made by the subject of personal data publicly available;
- that constitutes only last name, first name and patronymic of the subject of personal data;
- necessary for the purposes of a single access authorization of the subject of personal data to the territory where the owner and / or operator is located, or for other similar purposes;
- included in personal data information systems with the status of state automatized information systems;
- processed without the use of automation technology;
- processed in accordance with labour laws.

DATA PROTECTION OFFICERS

According to the Law on Personal Data, government bodies, legal entities and individuals processing personal data (i.e. **operators of personal data**) or having the right to use and dispose personal data (i.e. **owners of personal data**) must designate a structural unit or a responsible person that has to organize work with respect to personal data protection in the course of its processing.

COLLECTION & PROCESSING

Under the Law on Personal Data, processing of personal data includes actions with respect to:

- Collection;
- Systematization;
- Storage;
- Modification;
- Addition;
- Use;
- Provision;
- Dissemination;
- Transfer;
- Depersonalization; and
- Destruction.

Further, the Law on Personal Data stipulates 7 grounds / conditions for processing of personal data, as follows:

- upon the subject’s consent to processing of his / her personal data;
- when processing of the subject’s personal data is necessary to fulfil the agreement to which the subject is a party to, or to take measures at the request of the subject before concluding such agreement;
- when processing of the subject’s personal data is required for fulfilment of obligations of the owner and / or operator as defined by law;
- when processing of the subject’s personal data is necessary for protection of legitimate interests of the subject or other person;

- when processing of the subject’s personal data is required to exercise the rights and legitimate interests of the owner and / or operator or a third party, or in order to achieve socially significant goals, provided that the subject’s rights are not violated;
- when processing of the subject’s personal data is necessary for statistical or other research purposes, under the mandatory condition of depersonalization of personal data;
- if the subject’s personal data is taken from public sources.

Processing of personal data should pursue a certain purpose. This purpose should be fixed in legal acts, regulations, charter or other documents regulating the activities of the owner / operator of personal data. That said, the owner / operator should specify in its foundation documents or other internal documents (e.g. data privacy policy etc.) the purpose of data processing. Whenever the purpose of these operations changes, a new consent from the subject to conduct operations over the personal data related to them in line with such new purpose must be obtained.

In order to achieve the intended purpose of personal data processing, the owner / operator has the right to independently determine the procedure and principles of collection and systematization of personal data. Therefore, the volume and the nature of personal data to be processed should correspond to the purpose and applied methods of processing.

According to the Law on Personal data, the owner / operator may assign the processing of personal data to third parties in the following cases:

- upon the subject’s consent obtained in a written form or in the form of an electronic document;
- if such assignment is made based on an agreement between the owner and the subject of personal data or for the fulfilment of the conditions of an existing agreement;
- other cases stipulated by law.

In processing the personal data, the owner / operator must comply with notification requirements set by the Law on Personal Data. Under the foregoing Law, the owner / operator must notify the subject:

- on inclusion of the subject’s personal data into the personal database along with informing the subject on purpose of personal data processing and the subject’s respective rights. The period of notification is not defined by the Law on Personal Data;
- on transfer of the subject’s data to third parties. Such notification must be provided within a 3-day period;
- upon the subject’s application. Under the Law on Personal Data, the subject has the right to request the owner / operator to provide him / her with information about processing of his / her data.

Upon achievement of the processing purpose, as well as in other cases stipulated by the Law on Personal Data (e.g. withdrawal of the subject’s consent, decision of the court etc.) personal data is subject to destruction by the owner / operator.

Along with the above, on 15 January 2021 data localization requirement was introduced to the Law on Personal Data that came into force on 16 April 2021. Under this requirement the personal data of Uzbek citizens processed with the use of information technologies, including via the Internet, must be collected, systematized and stored on technical means physically located on the territory of Uzbekistan and in databases duly registered in the State Register of Personal Databases.

TRANSFER

The Law on Personal Data defines the cross-border transfer of personal data as the transfer of personal data by the owner / operator outside the territory of the Republic of Uzbekistan. Cross-border transfer of personal data is allowed only to the territory of foreign states providing adequate protection of the rights of personal data subjects. At present, it is unclear which states will qualify as providing “adequate” protection, as no list of such countries has been adopted yet by the regulatory authorities.

Nevertheless, cross-border transfer of personal data is still possible even if the foreign state does not provide the adequate protection. Such transfer is possible in 3 exceptional cases:

- the subject explicitly agrees to such transfer;

- there is a need to protect the constitutional order of Uzbekistan, the public order, rights and freedoms of citizens, health and morality of the population;
- if such transfer is stipulated by the international treaty of Uzbekistan.

The Law on Personal Data also determines that cross-border transfer of personal data may be prohibited or restricted in order to protect the constitutional order of the Republic of Uzbekistan, morality, health, rights and legitimate interests of citizens, and to secure defense of the country and national security.

SECURITY

The Law on Personal Data states that personal data is subject to the protection guaranteed by the State. It also imposes obligations on the owner / operator of personal data and the third party acquiring personal data to take necessary legal, organizational and technical measures ensuring:

- non-interference into the subject's private life;
- integrity and safety of personal data;
- confidentiality of personal data;
- prevention of illegal processing of personal data.

Obligations of the owner / operator of personal data on protection of confidentiality of personal data arise from the moment such data is collected until their destruction or depersonalization.

The owner / operator of personal data shall take organizational and technical measures to protect personal data based on the potential threats to their security.

Threats to the security of personal data are defined as a combination of conditions and factors that may lead to their alteration, addition, use, provision, transfer, dissemination, depersonalization, destruction, and copying as a result of unauthorized, including accidental access to the personal database.

Please note that the recently adopted Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 570 ‘On Approval of Certain Normative Legal Documents in the Field of Processing of Personal Data’ dated 5 October 2022 approved the following regulations that came into effect on 7 January 2023:

- the Regulation on determining the levels of protection of personal data during their processing;
- the Regulation on the requirements for material carriers of biometric and genetic data and storing technologies of such data outside personal databases.

BREACH NOTIFICATION

There is no requirement on breach notification under the Law on Personal Data. However, in case of violation of data processing rules (e.g. unauthorized data processing), the owner / operator of personal data must suspend processing of personal data or destroy them.

ENFORCEMENT

Following the adoption of the Law on Personal Data, a number of amendments aimed at enforcing data protection rules, were introduced into the Code on Administrative Liability and Criminal Code.

Currently, under the Code of Administrative Liability illegal collection, systematization, storage, modification, addition, use, provision, dissemination, transfer, depersonalization and destruction of personal data, as well as non-compliance with the localization requirement leads to the imposition of an administrative fine on citizens in the amount of 7 base calculation values (“**BCV**”) (approx. USD 193) and on officials – in the amount of 50 BCV (approx. USD 1,382).

Repeated violation of data protection rules can lead to criminal liability. Under the Criminal Code illegal processing of personal data leads to the fine in the amount from 100 BCV to 150 BCV (approx. from USD 2,764 to USD 4,146), or deprivation of a certain right for up to 3 years, or correctional labour for up to 2 years.

Furthermore, under Resolution No. 707, non-compliance with localization requirement leads to inclusion of an owner / operator of personal data into the Register of Infringers of the Rights of Personal Data Subjects and blocking access to the information resources (web-sites) of an owner / operator of personal data in Uzbekistan.

Apart from the above, the Personalization Agency can issue binding orders to legal entities and individuals on elimination of violations of data protection requirements.

ELECTRONIC MARKETING

The Law on Personal Data does not specifically regulate the use of personal data in electronic marketing. However, considering that the Law on Personal Data applies to any processing of personal data this Law will also cover processing of personal data in electronic marketing.

In addition to the above, the Law of the Republic of Uzbekistan No. ZRU-792 ‘On E-Commerce’ dated 29 September 2022, coming into effect on 31 December 2022, stipulates that the terms of use of personal data in e-commerce trading may be contractually agreed by e-commerce participants.

Lastly, the Law of the Republic of Uzbekistan No. ZRU-776 “On Advertisement” (new edition) adopted 7 July 2022 and entered into force on 9 September 2022, introduced new rules for dissemination of advertisements via telecommunication networks. A prior consent of a person is now required for distribution of advertisements through telecommunication networks. Given that telecommunication networks are broadly defined by law, it is most likely that such networks also include Internet and, therefore, this rule shall also apply to distribution of advertisements via Internet.

ONLINE PRIVACY

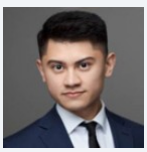
Current data protection laws do not provide for regulation of online privacy. However, if personal data is involved and privacy issues are concerned, there are no obstacles for their application with respect to online privacy.

KEY CONTACTS

Centil Law Firm
centil.law/#

Dilshad Khabibullaev
Partner
Centil Law Firm
T +998711204778
dilshad.k@centil.law

Valeriya Ok
Senior Associate
Centil Law Firm
T +998711204778
valeriya.ok@centil.law



Islam Gulomov
Senior Associate
Centil Law Firm
T +998711204778
islam.g@centil.law

Ibrokhim Musakhodjaev
Associate
Centil Law Firm
T +998711204778

ibrokhim.musakhodjaev@centil.law

DATA PRIVACY TOOL

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