LEGAL ALERT

KOSTA LEGAL

ADOPTION OF DATA PROTECTION LAW

16 July 2019

On June 2, 2019, the Law on Personal Data (the "**Law**") has been adopted. Unofficial English version of the Law can be found at: https://kostalegal.com/publications/law-of-the-republic-of-uzbekistan-on-personal-data. The Law shall come into force on October 1, 2019. It means that, by that date, all organizations have to change the way they capture, use and share personal data – both internally and externally – regardless their size or structure. The issues concerning the cross - border transfers of personal data are also covered by the Law. Thus, it shall apply to all Uzbekistan-based companies, irrespective of whether personal data is processed inside or outside of the Uzbekistan. This review aims to clearly map the obligations of the private-sector organizations when processing personal data and list practical implications of the Law.

The purpose of the Law is to regulate relations in the area of personal data protection. In this regard, the standards for gathering, processing and storing personal data for data controllers has been set. The State Center for Personalization under the Cabinet of Ministers (the "**Center**") is appointed as the authorized body in the area of personal data protection.

As the Law stipulates, the term "*personal data*" shall mean any information relating to a specific or identifiable individual recorded on electronic, paper and (or) other tangible carriers. An individual to whom personal data belong is regarded as a data subject (*subject*). Individuals, organizations, and companies that are either *possessors* or *operators* of personal data are going to be covered by the Law. Operators are the ones who are processing the personal data, whereas the possessors are the ones who own the databases.

The Law shall not be applicable to personal data processing performed by individuals for their personal use and not related to professional or commercial activities.

KEY AUTHORITIES

According to the Law, the personal data regulation in Uzbekistan is centered on the following government authorities:

- the Cabinet of Ministers – adopts (i) the legislative acts in the area of personal data protection, including the procedure for maintaining the State Register of Personal Data Databases (hereinafter – the "**Register**"), (ii) requirements for security levels of personal data contained in both electronic and tangible carriers;
- the Center – among other powers, has the authority to (i) approve the Standard Procedures for the processing personal data, (ii) maintain the Register, (iii) issue a

40a, Mustaqillik ave.,
Tashkent, 100000, Uzbekistan
+998 71 209 02 40
www.kostalegal.com

certificate of databases registration, (iv) determine the required level of personal data security, (v) give legal entities and individuals mandatory instructions (vi) cooperate with the competent authorities of foreign countries and international organizations in the area of data protection.

CONCEPT OF PERSONAL DATA

The Law specifies the following categories of personal data: sensitive or 'special category data', biometric and genetic.

According to the Law, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, political party and trade-union membership, health-related data (physical and mental health), data concerning a person's private life or criminal record are considered 'special'. Special category data is subject to specific processing conditions.

Further, the Law defines *biometric data* as 'personal data relating to the anatomical and physiological characteristics of a subject'. Whereas, *genetic data* are 'personal data relating to the inherited or acquired genetic characteristics of a subject, which result from the analysis of a biological sample or from the analysis of another element enabling equivalent information to be obtained.'

The Law specifically singles out these categories of personal information, so the possessors and/operators will need to identify the risks the processing of such specific data presents to data subjects and implement measures tailored to mitigate those risks.

PROCESSING OF PERSONAL DATA

Under the Law, *data processing* includes the implementation of one or a set of actions for the collection, systematization, storage, modification, addition, use, provision, dissemination, transfer, depersonalization and destruction of personal data. The processing of depersonalized data does not trigger the application of data protection law.

The Law establishes a rule that makes processing dependent on data subject consent. The cases related to the implementation of international treaties of the Republic of Uzbekistan, the administration of justice, enforcement proceedings are exempted from this rule.

Thus, there is a clear responsibility for organizations to obtain a consent from people they collect information about. The request for a consent must be given in an easily accessible form and shall clearly indicate the purpose of such processing. In cases, when the initial purpose for data processing changes, an additional consent shall be obtained. It is to note that the purpose of data processing shall be consistent with the rights and obligations of the possessor and/or operator. In other words, the purpose shall necessarily be in line with the company's primary activities.

The consent must be clear and distinguishable from other matters. The validity period of the consent

shall also be expressly indicated. The consent may be provided in any form that allows to confirm the fact of its receipt. The Law also allows for the electronic form of the consent.

As a general rule, the Law prohibits processing of special category data. However, exceptions are provided. In addition to all exceptional cases stipulated in the Art.25 of the Law, such processing is possible given that the data subject provides the explicit consent in both written and electronic forms.

ACCOUNTABILITY AND COMPLIANCE

Companies covered by the Law are accountable for their handling of people's personal information. Such companies guarantee adequate security of personal data and strict adherence to confidentiality.

Databases

The Law imposes an obligation on companies to register their personal data databases with the Center. To
register a database, an application shall be filed with the Center. The Law does not provide for a detailed procedure on the registration, but establishes that the Cabinet of Ministers adopts the procedure for registration of databases. We believe that the relevant subordinate legislation governing the registration issues will shortly be adopted.

As per the Law, after the registration a possessor and/or an operator has an obligation to notify the Center about all changes in the information initially provided by the applicant to register the particular database within 10 days as of the day the change occurred. The Law is silent as to this information.

Notably, the databases containing the following information shall not be subject to registration:

- only on a surname, first name and patronymic of individuals;
- personal data, which are publicly available;
- personal data that are processed without the use of automation and/or in accordance with labor legislation.

Notification procedure

Companies shall have to give users more control over their data. There are certain exceptions[1], but generally, people must be provided with an explanation on a decision made about their personal data. This includes the notification of the data subject of company's actions during processing (e.g. transfer of the data to third parties). Such a notification is provided by companies in written form within 3 working days. The notification is not required, if the data is transferred for historical, statistical, sociological or scientific purposes or the data transferred is publicly available.

1. Processing of personal data obtained during investigations relating to potentially illegal activity/ violation of third party's rights and/or interests.

Data erasure

There are also provisions that resembles the well - known '*right to be forgotten*'. Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes of processing, or a data subject withdrawing consent. It should also be noted that this right may require controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests[1].

Cross-border transfers

Companies shall be conducting data mapping to identify all cross-border transfers of personal data, so that they can determine the best way to comply with the Law. Any transfer of personal data to a third country can take place, only if certain conditions are met by the data exporter and the data importer. Cross-border transfers may take place without a need to obtain authorization, if the third country's national law ensures an adequate level of protection for personal data. In the absence of an adequacy determination, a cross-border transfer can still take place, provided that the data subject explicitly consents to such transfer.

RIGHTS OF DATA SUBJECT

In addition to imposing new obligations on the companies and organization's collecting personal data, the Law also gives individuals a lot more power to access the information that is held about them. Everyone shall have a right to get confirmation that an organization has information about them, access to this information and any other supplementary information. Furthermore, individuals are also entitled no to provide explanations and reasons for their refuse to disclose their personal information.

Additionally, the Law tackles issues concerning the potential negative outcomes of algorithmic (automatic) decision-making/automated processing of personal data. The data subject shall have the right not to be subject to solely automatic decision-making, which produces legal effects concerning him/her, or affects his/her rights and legitimate rights (e.g. an online decision to award a loan, profiling, worker's pay is linked to their productivity monitored automatically). The Law allows automatic decision-making only provided that (i) it is necessary for the performance of a contract between the data subject and a possessor or (ii) it is based on the data subject's explicit consent in both written and electronic forms. In this regard, data subject shall have the right to contest a decision made based on solely automated data processing (excludes any human influence on the outcome). The possessor and/or the operator is obliged to consider the objection and to inform the data subject of the outcome in written form within 10 days.

NON-COMPLIANCE

The relevant addendums to the Code on Administrative Liability and Criminal Code have also been introduced recently. These addendums clarify what kind of liabilities are set for infringements of data protection law.

[1] The scope of data protection law does not extend to the cases of data processing related to investigative, intelligence and counterintelligence activities, the fight against crime, law enforcement, as well as to the cases of money laundering combating.

As per addendums to the Code on Administrative Liability, fines for relevant infringements may now be imposed on both individuals and managers of legal entities in the following manner:

- for managers - illicit data processing entails imposition of a fine in the amount of 5-10 minimum monthly wages (MMW) (UZS 1,013,650 – UZS 2,027,300 or approx. USD 119 – USD 238);
- for individuals - illicit data processing entails imposition of a fine in the amount of 3-5 MMW (UZS 608,190 – UZS 1,013,650 or approx. USD 72 – USD 119).

The addendums introduced to Criminal Code establish criminal liability for the illicit data processing, if it is committed after the imposition of an administrative penalty in the form of a fine up to 50 times MMW (UZS 10,136,500 or approx. USD 1,186) or temporary deprivation of certain right for up to 3 years or community work for up to 2 years. If such an offence is committed in the presence of aggravating circumstances, it attracts a fine between 50 and 100 MMW or community work for 2 to 3 years or deprivation of liberty for 1 to 3 years.

The following circumstances are considered aggravating:

- commission of the offence by a group of persons acting in conspiracy;
- commission of the offence with the abuse of one's official position;
- commission of the offence involving serious consequences;
- commission of the offence out of mercenary or other base motives;
- commission of the offence repeatedly or by a dangerous recidivist.