Uzbekistan | December 2022

STRENGTHENING REQUIREMENTS FOR THE DATA PROTECTION

On October 5, 2022, the Cabinet of Ministers of the Republic of Uzbekistan (hereinafter – "**Uzbekistan**") adopted the Resolution "On the Approval of Certain Regulatory Legal Acts in the Field of Personal Data Processing" No. 570 (hereinafter – the "**Resolution**"). The Resolution will come into force on January 7, 2023. Please see below some of the key, from our standpoint, changes provided by the Resolution.

The Resolution introduces the following Regulations:

- on determining the level of protection of personal data (hereinafter – the "**PD**") while its processing (hereinafter – the "**Regulation No. 1**");
- on the requirements for physical media with biometric and genetic data and technologies for storing the data outside the PD databases (hereinafter – the "**Regulation No. 2**").

The Regulation No. 1

The Regulation No. 1 determines threats to the PD security while the PD is processed by the owner and (or) the operator of the PD database, levels of the PD protection and the necessary measures to ensure the PD protection. Threats to the PD security are defined as a set of conditions and factors that may cause alteration, supplementation, use, provision, transfer, distribution, depersonalization, destruction, copying of the PD as a result of unauthorized, including accidental access to the PD database.

Threats are classified into the following three types depending on the presence of undocumented (undeclared) features in system and application software of the PD databases:

i. Threats related to the presence of undocumented (undeclared) features in the PD database system software;
ii. Threats related to the presence of undocumented (undeclared) features in the PD database application software;
iii. Threats not related to the presence of undocumented (undeclared) features in system and application software of the PD database.

Furthermore, the Resolution defines 4 levels of the PD protection which shall be ensured by the owner and (or) operator of the PD databases while processing in the PD databases. The level of protection that should be provided is determined based on the existence of some conditions. For

instance, the **1st level** of the PD protection shall be ensured if at least one of the following conditions exists:

- type 1 threats and processing of special PD[1] and (or) biometric and (or) genetic data;
- type 2 threats and processing of special PD of more than 50 thousand individuals who are not employees of the owner and (or) operator of the PD database.

The **2nd level** of protection shall be ensured if at least one of the following conditions exists:

- type 1 threats and processing of publicly available information;
- type 2 threats and processing of the employees special PD, and special PD of less than 50 thousand subjects who are not employees of the owner and (or) operator;
- type 2 threats and processing of biometric and (or) genetic data;
- type 2 threats and processing of publicly available information of more than 50 thousand subjects who are not employees of the owner and (or) operator;
- type 3 threats and processing of special PD of more than 50 thousand subjects who are not employees of the owner and (or) operator.

The **3rd level** of protection shall be ensured if at least one of the following conditions exists:

- type 2 threats and processing of publicly available information of: (i) employees of the owner and (or) operator, (ii) less than 50 thousand subjects who are not employees of the owner and (or) operator;
- type 3 threats and processing of special PD: (i) employees of the owner and (or) operator, (ii) less than 50 thousand subjects who are not employees of the owner and (or) operator;
- type 3 threats and processing of biometric and (or) genetic data.

The **4th level** of protection shall be ensured when processing publicly available information and if type 3 threats exist.

The Regulation No. 2

The Regulation No. 2 stipulates requirements for technologies storing biometric and genetic data outside of the PD databases, as well as for physical media with the data.

[1] Special PD – the data on racial or social origin, political, religious or ideological beliefs, membership of political parties and trade unions, as well as data concerning physical or mental health, information about private life and criminal record (Article 25 of the Law of Uzbekistan "On Personal Data" № ZRU-547 dated July 02, 2019).

Among the main requirements, we can highlight the requirement of mandatory marking the physical media used to process biometric and genetic data as “Secret” or “Restricted”.

According to the Regulation No. 2 biometric and genetic data may only be stored electronically in encrypted form using cryptographic or other protection means. Also, when storing biometric and genetic data outside of the PD databases, following requirements must be met:

- Access to the PD stored on physical media must be provided to authorized persons of the owner and (or) operator of the biometric and genetic database;
- Use of electronic digital signatures (e-signatures) or other information technologies to preserve the integrity and invariability of biometric and genetic data recorded on physical media.
- Verification of the subject's written consent to the processing of biometric and genetic data or presence of other grounds for their processing provided for by law.

Contacts:

Zafar Vakhidov — Partner, Vakhidov & Partners
Uzbekistan / Kazakhstan
ZV@vakhidovlaw.com

Fatkhulla Nigmanov — Associate, Vakhidov & Partners
Uzbekistan
FatkhullaN@vakhidovlaw.com