

Kazakhstan – August 2026

Amendments to Kazakhstan Laws on Digitalization and Personal Data

On 24 June 2026, the Law No. 326-VIII "On Introduction of Amendments and Supplements to Certain Legislative Acts on Digitalization, Personal Data Protection, Road Traffic, and the Regulation of Advanced Technologies in Transportation" (hereinafter referred to as the "**Amendments Law**") was adopted in the Republic of Kazakhstan (hereinafter referred to as "**Kazakhstan**").

On 25 June 2026, the Amendments to Law were officially published. They will generally enter into force on 25 August 2026, except for certain provisions that entered into force on 12 July 2026. Certain other provisions will enter into force on 1 January 2027 and 1 January 2029.

We will focus below on the most significant amendments introduced to the Law of Kazakhstan No. 94-V dated 21 May 2013, "On Personal Data Protection" (hereinafter referred to as the "**Personal Data Protection Law**").

The Personal Data Protection Law has been amended as follows:

The following new terms are defined:

- deletion of personal data;
- anonymization of personal data;
- masking of personal data;
- disclosure of personal data in publicly available sources;
- the Register of Personal Data Controllers and/or Processors;
- a digital object containing personal data;
- a personal data identifier;
- the Register of Personal Data Security Breaches;
- a personal data security breach;
- hashing of digital data.

The purposes for which personal data identifiers are used, as well as what constitutes a personal data identifier, are now specified.

Personal data identifiers are used to identify a data subject in connection with both publicly available personal data and personal data with restricted access.

Personal data identifiers include:

1. the data subject's surname, first name, and patronymic (if indicated in the identity document), taken together;
2. the individual identification number (IIN);
3. an image of the data subject's face;
4. the data subject's facial biometric vector or its derivatives, where these derivatives can be reconstructed to their original values.

Data controllers and/or data processors, as well as third parties that process personal data, have been classified.

Data controllers and/or processors, as well as third parties that collect and process personal data, are classified as small, medium, or large entities based on the volume of personal data they collect and process.

For the purposes of determining the volume of personal data processed, the total number of unique data subjects whose personal data is processed by a data controller, data processor, or third party across one or more digital objects is taken into account.

The criteria for classifying data controllers, data processors, and third parties that process personal data as small, medium, or large entities apply irrespective of their legal form, ownership structure, or type of activity.

For the purposes of the classification:

- **small entities** are data controllers and/or data processors, as well as third parties, that collect and process the personal data of no more than 10,000 (ten thousand) unique data subjects;
- **medium-sized entities** are those that collect and process the personal data of more than 10,000 (ten thousand) but fewer than 500,000 (five hundred thousand) unique data subjects; and
- **large entities** are those that collect and process the personal data of 500,000 (five hundred thousand) or more unique data subjects.

The competence of the Ministry of Artificial Intelligence and Digital Development of Kazakhstan was expanded.

The competence of the Ministry of Artificial Intelligence and Digital Development of Kazakhstan now also includes:

1. maintaining the Register of Personal Data Controllers and/or Processors;
2. maintaining the Register of Personal Data Security Breaches involving personal data processed without the consent of the data subject or the data subject's legal representative.

A new provision was introduced establishing the procedure for notifying the commencement and termination of personal data processing.

Large data controller and/or data processor, as well as any third party that processes personal data, must notify the Ministry of Artificial Intelligence and Digital Development of Kazakhstan of their intention to commence and to cease the processing of personal data before this processing begins and before it is terminated.

The notification must be submitted in writing, whether in paper or electronic form or another tangible medium, and must be signed by an authorized representative.

A Register of Personal Data Security Breaches was established.

The Register of Personal Data Security Breaches is maintained by the Ministry of Artificial Intelligence and Digital Development of Kazakhstan on the basis of information received from publicly available sources, as well as from cybersecurity operations centres, sectoral cybersecurity centres, the State Cybersecurity Operations Centre, the Cybersecurity Incident Response Service, the National Cybersecurity Coordination Centre, and the National Computer Incident Response Service.

The Ministry of Artificial Intelligence and Digital Development of Kazakhstan maintains the Register of Personal Data Security Breaches by recording incidents in which third parties have obtained unauthorized access to personal data without the consent of the data subject or the data subject's legal representative.

VAKHIDOV & PARTNERS

vakhidovlaw.com

Contacts:



Zafar Vakhidov

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



Almas Tleupov

Associate, Vakhidov &
Partners
Kazakhstan
AlmasT@vakhidovlaw.com

+7 705 209 91 59 | +998 97 727 0345
zv@vakhidovlaw.com
vakhidovlaw.com