On approval of the Rules for implementation by owner and (or) operator, as well as third party of measures to protect personal data

Invalidated Unofficial translation

Decree of the Government of the Republic of Kazakhstan № 909 dated September 3, 2013. Abolished by the Decree of the Government of the Republic of Kazakhstan dated 07/13/2023 No. 559

Unofficial translation

Footnote. Abolished by the Decree of the Government of the Republic of Kazakhstan dated 07/13/2023 No. 559 (effective from the date of its first official publication)

In accordance with Subparagraph 4) of Article 26 of the Law of the Republic of Kazakhstan dated May 21, 2013 “On personal data and their protection”, the Government of the Republic of Kazakhstan **hereby DECREES AS FOLLOWS**:

1. Approve the attached Rules for implementation by owner and (or) operator, as well as third party of measures to protect personal data.

2. This Decree shall be enforced from November 25, 2013 and to be subject to official publication.

The Prime Minister
of the Republic of Kazakhstan *S. Akhmetov*

Approved by
the Decree of the Government of
the Republic of Kazakhstan
No. 909 dated September 3, 2013

Rules for implementation by owner and (or) operator, as well as a third party of measures to protect personal data

Footnote. The Rules are as amended by the Decree of the Government of the Republic of Kazakhstan dated 18.01.2021 No. 12 (shall be enforced upon expiry of ten calendar days after the date of its first official publication).

Chapter 1. General Provisions

1. These Rules for implementation by owner and (or) operator, as well as a third party of measures to protect personal data (hereinafter referred to as the Rules) have been developed in accordance with Subparagraph 4) of Article 26 of the Law of the Republic of Kazakhstan dated May 21, 2013 “On personal data and their protection" (

hereinafter referred to as - the Law) and determine the procedure for owner and (or) operator, as well as a third party, to take measures to protect personal data.

2. The following basic concepts shall be used in these Rules:

1) personal data – details, related to the subject of personal data, specific or defined on their basis, recorded on an electronic, paper and (or) other physical media;

2) blocking of personal data – actions on temporary termination of collection, accumulation, change, supplement, use, distribution, depersonalization and destruction of personal data;

3) collection of personal data – actions, directed to reception of personal data;

4) destruction of personal data – actions, in the result of commission of which is impossible to restore the personal data;

5) depersonalization of personal data – actions, in the result of commission of which determination of belonging of personal data to the subject of personal data is impossible;

6) a database containing personal data (hereinafter referred to as - the database) is a set of ordered personal data;

7) owner of a database containing personal data (hereinafter referred to as - owner) - a state authority, individual and (or) legal entity that, in accordance with the laws of the Republic of Kazakhstan, exercise the right to own, use and dispose of a database containing personal data;

8) operator of a database containing personal data (hereinafter referred to as - operator) - a state authority, individual and (or) legal entity that collects, processes and protects personal data;

9) protection of personal data - a set of measures, including legal, organizational and technical, carried out for the purposes established by the Law;

10) authorized body in the field of personal data protection - a central executive body in charge for personal data protection;

11) processing of personal data – actions, directed to accumulation, storage, change , supplement, use, distribution, depersonalization, blocking and destruction of personal data;

12) a subject of personal data (hereinafter – subject) – individual, to which the personal data are referred;

13) public available personal data - personal data or information, which, in accordance with the Laws of the Republic of Kazakhstan, shall not be subject to confidentiality requirements, access to which is free with the consent of the subject;

14) Personal data of limited access – the personal data, an access of which is limited by the legislation of the Republic of Kazakhstan;

15) third party - a person who is not a subject, owner and (or) operator, but related to them (him/her) by circumstances or legal relations for collection, processing and protection of personal data;

16) electronic information resources – information in electronic digital form contained on an electronic medium and in informatization facilities.

17) a survey of securing the processes of storage, processing and distribution of personal data of restricted access contained in electronic information resources (hereinafter referred to as the survey) - an assessment of the security measures and protective actions applied in the processing, storage, distribution and protection of personal data of restricted access contained in electronic information resources.

Other concepts, used in these Rules, shall apply in accordance with the Law and the Law of the Republic of Kazakhstan dated November 24, 2015"On Informatization" .

Footnote. Paragraph 2 as amended by the Resolution of the Government of the Republic of Kazakhstan dated 30.04.2021 No. 285 (shall be enforced upon expiry of ten calendar days after the date of its first official publication); dated 26.10.2022 No. 849 (shall enter into force upon expiry of ten calendar days after the day of its first official publication).

Chapter 2. The procedure for implementation by owner and (or) operator as well as third party measures to protect personal data

3. Owner and (or) operator, as well as third parties are obliged to take necessary measures to protect personal data, ensuring:

1) prevention of unauthorized access to personal data;

2) timely detection of unauthorized access to personal data if such unauthorized access could not be prevented;

3) minimizing the adverse effects of unauthorized access to personal data;

4) granting access to the state technical service to informatization objects that use, store, process and distribute personal data of restricted access contained in electronic information resources, in order to conduct a survey in accordance with the rules for conducting a survey on ensuring the security of storage, processing and distribution of personal data of restricted access contained in in electronic information resources approved by the authorized body;

5) registration and accounting of actions provided for by Article 8, paragraph 4, subparagraphs 3), 4), 5), 6) of the Law.

Footnote. Paragraph 3 as amended by the Resolution of the Government of the Republic of Kazakhstan dated 30.04.2021 No. 285 (shall be enforced upon expiry of ten calendar days after the date of its first official publication); dated 14.04.2022 No.

219 (shall enter into force upon expiry of ten calendar days after the day of its first official publication).

4. Threats to the security of personal data shall be understood as a set of conditions and factors that create the possibility of unauthorized, including accidental, access to personal data during their collection and processing, which may result in destruction, alteration, blocking, copying, unauthorized provision to third parties, unauthorized distribution of personal data, as well as other illegal actions.

5. Personal data protection shall be carried out by applying a set of measures, including legal, organizational and technical, in order to:

1) exercise of privacy rights, personal and family secrets;

2) ensuring integrity and safety;

3) observance of their confidentiality;

4) exercise of the right to access them;

5) prevention of illegal collection and processing thereof.

6. Obligations of the owner and (or) operator, as well as of a third party to protect personal data arise from the moment of collection of personal data and shall be valid until their destruction or depersonalization.

7. To ensure protection of personal data, it is necessary:

1) to allocate business processes, containing personal data;

2) to separate personal data to generally accessible and of limited access;

3) determining a list of persons, who perform the collection and processing of personal data, or having access to them;

4) appointment of a person responsible for organizing the processing of personal data if the owner and (or) operator are legal entities. The obligations of the person responsible for organizing the processing of personal data are specified in Paragraph 3 of Article 25 of the Law. The effect of Subparagraph 4) of this paragraph shall not apply to the processing of personal data in the activities of the courts.

5) establishment of the procedure of access to personal data;

6) approval of documents defining the operator's policy regarding the collection, processing and protection of personal data;

7) at the request of the authorized body, within the framework of consideration of appeals from individuals and legal entities, provide information on the methods and procedures used to ensure compliance by the owner and (or) operator with the requirements of the Law.

When collecting and processing personal data at the informatization facilities, it is necessary to ensure additionally the safety of personal data storage media.

Footnote. Paragraph 7 as amended by the resolution of the Government of the Republic of Kazakhstan dated 14.04.2022 No. 219 (shall enter into force upon expiry of ten calendar days after the day of its first official publication).

8. Other particularities of personal protection data when collecting and processing thereof at the informatization facilities shall be established in accordance with the legislation of the Republic of Kazakhstan on informatization.

9. Owner and (or) operator when processing personal data of limited access shall:

1) establish the purposes of processing personal data of limited access. Personal data of limited access shall be used in accordance with the declared purposes.

2) determine the procedures of processing, distribution and access to personal data of limited access;

3) determine the procedures of blocking personal data of limited access related to the subject, upon request of the subject.

Owner and (or) operator as well as the third party when processing personal data of limited access shall:

1) determine the list of persons who have access to personal data of limited access;

2) notify the authorized body in the field of personal data protection about incidents of information security, associated with illegal access to personal data of limited access ;

3) ensure the installation of information security tools, software updates on technical means that process the personal data of limited access;

4) ensure keeping the log of events of database management systems;

5) ensure keeping the log of actions of users who have access to personal data of limited access;

6) use tools to control the integrity of personal data of limited access;

7) ensure the transfer of personal data of limited access to other persons through secure communication channels and (or) using encryption and with the consent of the subject of personal data, unless otherwise provided by the legislation of the Republic of Kazakhstan;

8) allocate business processes containing personal data of limited access;

9) ensure the use of means of cryptographic protection of information for the reliable storage of personal data of limited access;

10) use means of identification and (or) authentication of users when working with personal data of limited access.

10. Collection and processing of personal data of limited access shall be carried out through the informatization facilities, placed in the territory of the Republic of Kazakhstan.

Storage and transfer of personal data of limited access shall be carried out using the means of cryptographic protection of information, having parameters not lower than the third security level in accordance with the Standard of the Republic of Kazakhstan ST RK 1073-2007 “Cryptographic information protection means. General technical requirements ".

The requirements of this clause shall not apply to cases of cross-border data transfer.

© 2012. «Institute of legislation and legal information of the Republic of Kazakhstan» of the Ministry of Justice of the Republic of Kazakhstan