

**Annex to the Order of  
Kazakhtelecom JSC dated October  
18, 2021 No. 284**

**Personal Data Protection Policy in Kazakhtelecom JSC**

Almaty, 2021

## **Table of contents**

<b>1. Terms, abbreviations and definitions .....</b>	<b>3</b>
<b>2. General regulations .....</b>	<b>4</b>
<b>3. Main purposes and objectives.....</b>	<b>4</b>
<b>4. Collection, processing and protection of personal data.....</b>	<b>5</b>
<b>5. Blocking, depersonalization, destruction of personal data .....</b>	<b>6</b>
<b>6. Transfer and storage of personal data .....</b>	<b>7</b>
<b>7. Access to personal data .....</b>	<b>8</b>
<b>8. The basic principles of ensuring the PDP .....</b>	<b>8</b>
<b>9. Roles and responsibilities .....</b>	<b>9</b>
<b>10. Final regulations .....</b>	<b>9</b>
<b>11. Annex .....</b>	<b>10</b>

## 1. Terms, abbreviations and definitions

**Blocking of personal data** — temporary termination of the collection, systematization, accumulation, use, dissemination of personal data, including their transfer.

«STS» JSC - "State Technical Service" Joint Stock Company.

**Personal Data Protection (PDP)** – a set of organizational and technical measures aimed at protecting personal data.

**IS** – information security.

**Information** — information (messages, data) regardless of the form of their presentation.

**Use of personal data** — actions (operations) with personal data performed by an employee of the Company for the purpose of making decisions or performing other actions necessary in the Company's business processes.

**ISC** – Information Security Committee.

**Confidentiality of personal data** — the obligation to prevent persons who have gained access to personal data from distributing them without the consent of the subject or other legal grounds.

**MDDIAI** – Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.

**RD** – regulatory documentation of the Company (policies, standards, orders, regulations, manuals, instructions, etc.).

**Depersonalization of personal data** — actions as a result of which it is impossible to determine whether personal data belongs to a specific subject.

**Processing of personal data** — actions (operations) with personal data, including collection, systematization, accumulation, storage, clarification (updating, modification), use, distribution (including transfer), depersonalization, blocking, destruction of personal data.

**Publicly available personal data** — personal data, access of an unlimited number of persons to which is provided with the consent of the subject or to which, in accordance with the laws of the Republic of Kazakhstan, the requirement of confidentiality does not apply.

**Company** – Kazakhtelecom Joint Stock Company.

**Personal data (PD)** — any information relating to an individual (subject of personal data) identified or determined on the basis of such information, recorded on electronic, paper and (or) other material media.

**Policy** – the present Policy on the protection of Personal data in Kazakhtelecom JSC approved by the Company.

**Dissemination of personal data** — actions aimed at transferring personal data to a certain circle of persons (transfer of personal data).

**SD** – structural division.

**SD IS** – structural division of information security;

**Destruction of personal data** — actions as a result of which it is impossible to restore the content of personal data in the personal data information system or as a result of which the material carriers of personal data are destroyed.

## 2. General regulations

1. The Personal data protection Policy of Kazakhtelecom JSC has been developed in order to define the basic principles of processing personal data of customers, suppliers, business partners, employees and others, and also defines the main actions for collecting, storing and processing personal data, measures for their protection in the Company.

2. The Policy is a fundamental document in the field of personal data protection, sets goals, objectives and principles in the field of PD protection, which guide the Company in its activities. Serves as a guide in the development of relevant personal data protection documents.

3. The regulatory and legal basis of this Policy is the Law of the Republic of Kazakhstan "On Personal Data and their Protection" (hereinafter - the Law), as well as the Rules for the Collection and Processing of Personal data approved by the Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated 21.10.2020 No. 395/NK and NSD of the Company.

4. All employees employed by the Company are required to familiarize themselves with this Policy under signature.

5. The Policy is a publicly available document that can be provided without restrictions to all interested parties.

### **3. Main purposes and objectives**

6. The main objectives that all the provisions of this Policy are aimed at achieving are:

- 1) continuity of PD availability to support the Company's business processes;
- 2) the integrity of PD in order to support the high quality of the Company's business processes;
- 3) confidentiality of PD;
- 4) compliance of the measures taken on the PDP applied in the Company with the requirements of the legislation of the Republic of Kazakhstan, as well as the requirements of regulatory and supervisory authorities.

7. The main tasks for the implementation of the Policy are planning, implementation and control over the implementation of a set of organizational and technical measures to ensure the PDP based on an assessment of the Company's risks in the field of information security, aimed at ensuring:

- 1) protection of PD from real and potential threats;
- 2) prevention, detection and deactivation of various threats;
- 3) establishing the causes and conditions of threats;
- 4) rapid response to the impact of modern threats and their precise localization;
- 5) minimizing damage from events that pose a threat to the safety of the PDP by preventing them or minimizing their consequences;
- 6) application of modern international methodologies and practices to improve the mechanisms of rapid response and investigation of threats;
- 7) effective information security risk management;
- 8) ensuring that employees are aware of the Policy, the measures taken, the requirements for ensuring the PDP, the duties and rules of conduct imposed on the Company's employees, as well as ensuring control over their proper implementation;

9) increasing the level of knowledge and development of corporate culture in the field of PDP;

10) improving the PDP;

11) ensuring compliance with the requirements of the legislation of the Republic of Kazakhstan in the course of activities to ensure the PDP in the Company.

8. In order to achieve these goals and solve the listed tasks, the Company is building a PDP that meets the requirements:

1) standards and legislation of the Republic of Kazakhstan in the field of PDP;

2) corporate regulatory documents, contractual obligations and other regulatory documents in the field of PDP.

The PDP, being part of the general management system of the Company, is documented in this Policy, as well as in other PDP documents (private policies, regulations, guidelines, standards, instructions, regulations, procedures, etc.), detailing and developing the provisions set out in this Policy at the level of their practical implementation and are mandatory for all employees of the Company, as well as representatives of third parties who have access to PD.

#### **4. Collection, processing and protection of personal data**

9. The procedure for obtaining (collecting) PD:

1) all PD of the subject shall be obtained from him personally with his written consent or his legal representative in the manner determined by the authorized body, except for the cases provided for in Article 9 of the Law;

2) the consent of the subject to the use of his PD is stored in paper form, in the subscriber's personal file;

3) the subject's consent to PD processing is valid for the entire duration of the subject's contractual relationship with the Company;

4) processing of PD of subjects without his consent is carried out in the following cases:

- PD are publicly available;

- at the request of authorized state bodies in cases provided for by the legislation of the Republic of Kazakhstan;

- PD processing is carried out for statistical purposes, subject to their mandatory depersonalization;

- in other cases provided for by Law.

10. PD processing procedure:

1) the PD subject provides the employee of the Company responsible for conducting operational work with information about himself;

2) based on the information received, the Company's employee checks the presence of this entity registered in the Company's information system. If the subject is absent from the information system of the Company, the operational employee enters the necessary information about the subject, after receiving the written consent of the latter. If there is information about the subject in the information system of the Company – checks the data with the previously provided (if necessary, makes appropriate changes);

3) PD processing of the subject can be carried out solely for the purpose of ensuring the implementation of business processes with the subject, in compliance with the legislation of the Republic of Kazakhstan and other regulatory legal acts;

4) the volume and content of processed PD shall be sufficient to perform business processes between the PD subject and the Company and not exceed this threshold.

5) The list of PD necessary and sufficient to perform the tasks performed shall be approved by the relevant administrative document for the Company where the data is processed, in accordance with the Annex to this Policy.

11. Personal data protection:

1) a subject's PDP is understood as a set of measures (organizational, administrative, technical) aimed at preventing illegal or accidental access to them, destruction, modification, blocking, copying, distribution of PD of subjects, as well as from other illegal actions on the part of persons who do not have access to PD;

2) The Company, in accordance with the legislation of the Republic of Kazakhstan, in the case of a PDP of subjects, it takes all the necessary organizational, administrative and technical measures, including:

- encryption (cryptographic) tools;
- antivirus protection;
- vulnerability analysis;
- access control;
- registration and accounting;
- organization of regulatory and methodological measures regulating the PDP.

## **5. Blocking, depersonalization, destruction of personal data**

12. The procedure for blocking and unblocking personal data:

1) blocking of PD of subjects is carried out with a written statement of the subject of personal data;

2) blocking PD implies:

- prohibition of PD editing;  
- prohibition of the distribution of PD by any means (e-mail, cellular communication, information media, etc.);

3) the blocking of the PD of the subject can be temporarily lifted if it is required to comply with the legislation of the Republic of Kazakhstan;

4) unblocking of the subject's PD is carried out with his written consent or application;

5) the repeated consent of the PD subject to the processing of his data entails the unblocking of his PD.

13. The procedure for depersonalization and destruction of PD is carried out on the basis of the decision of the Commission on Depersonalization and Destruction of PD (hereinafter - the Commission). The Commission is formed on the basis of the administrative document for the branch of the Company where PD was processed and shall consist of the Chairman of the Commission – an employee responsible for organizing PD processing and employees of the branch who have access to PD, in the number of at least 3 people. The Commission draws up an appropriate act, which is subsequently stored by the employee responsible for organizing the processing of PD in the Company's branch in a

separate folder. The depersonalization of the PD of the subject takes place for statistical, sociological, scientific, marketing research:

1) when depersonalizing PD in information systems, they are replaced by a set of characters, by which it is impossible to determine whether PD belongs to a specific subject;

2) PD are subject to destruction upon expiration of the PD storage period, upon termination upon termination of legal relations between the subject, the owner of the PD and the Company, upon entry into force of a court decision and in other cases established by Law and other regulatory legal acts of the Republic of Kazakhstan;

3) paper carriers of documents when depersonalizing PD are destroyed, also with the preparation of an appropriate act, which is subsequently stored by the employee responsible for organizing PD processing in the Company's branch in a separate folder;

4) the operation to depersonalize and destroy the PD of the subject is irreversible and cannot be restored.

## **6. Transfer and storage of personal data**

14. Transfer of personal data:

1) the transmission of a subject's PD is understood as the dissemination of information through communication channels and on material media;

2) when transferring PD, the Company's employees shall comply with the following requirements:

- transfer PD of subjects within the Company in accordance with this Policy, NSD and job descriptions;

- access to PD is allowed only to those employees with the appropriate level of access and volume who need PD to perform their official duties;

- transfer the PD of the subject to the legal representatives of the subject in accordance with the procedure established by the legislation of the Republic of Kazakhstan and NSD and limit this information only to those PD of the subject that are necessary for the specified representatives to perform their functions.

15. Storage and use of personal data:

1) PD storage refers to the existence of records in information systems and on material media;

2) PD is processed and stored in information systems, as well as on paper in the Company;

3) storage of restricted access PD in information systems is carried out in a database located on the territory of the Republic of Kazakhstan using cryptographic protection of information with parameters not lower than the third security level;

4) the storage period of PD is carried out no longer than the purposes of their collection and processing require, but not less than two years, after which the information is destroyed.

## **7. Access to personal data**

16. Granting access to the PD to the Company's employee is carried out in accordance with the approved Policy of managing access to information resources of Kazakhtelecom JSC. To do this, one of the following conditions shall be met:

- 1) access is necessary for the user to perform official duties in accordance with his job descriptions and powers;
- 2) access is necessary for the user to perform the duties of another user on behalf of (in the form of a memo) the head of the structural unit;
- 3) access is necessary for the user to perform the duties of another user at the direction (in the form of an order or order) of the Company's management;
- 4) access is necessary for the user to perform work on the instructions (in the form of an order or order) of the Company's management;
- 5) access is necessary for the user to perform work during the implementation of agreements/ contracts concluded by the Company (for representatives of third parties).

## **8. The basic principles of ensuring the PDP**

17. This Policy is based on the following basic principles:

- 1) observance of the constitutional rights and freedoms of man and citizen;
- 2) legality of the provision of a PDP;
- 3) confidentiality of restricted access PD;
- 4) involvement of the Company's management in the process of ensuring the PDP;
- 5) business orientation;
- 6) process approach;
- 7) integrated use of methods, methods and means of protection;
- 8) following best practices;
- 9) reasonable sufficiency;
- 10) awareness and personal responsibility.

## **9. Roles and responsibilities**

18. Control over the implementation of the requirements of this Policy, as well as for its relevance and amendments, is assigned to the SD IS.

19. Responsibility for ensuring proper compliance with the requirements of this Policy is assigned to all interested SD within their powers and in accordance with the provisions established by this Policy and documents developed on its basis.

20. SD managers are responsible for timely communicating the requirements of this Policy to employees of their divisions and/or representatives of third parties in the part concerning them, and for compliance by employees of their divisions and/or representatives of third parties with the requirements of this Policy.

21. All users shall be familiar with the requirements of this Policy.

22. All users are responsible for their actions when using PD in their work, as well as for meeting the requirements established by this Policy and internal documents developed on its basis.

23. In case of detection of violations of the requirements of this Policy, which entailed unauthorized access by unauthorized persons during the collection, storage, processing of PD, an internal investigation shall be initiated and conducted with the involvement of interested SDs, as well as representatives of «STS» JSC , ISC MDDIAI.



24. Failure to comply with the measures provided for in this Policy entails liability in accordance with the current legislation of the Republic of Kazakhstan and internal documents of the Company.

## **10. Final regulations**

25. The provisions of this Policy are subject to revision based on the results of an external audit, internal analysis and assessment of IS risks for the Company's information system, as a result of any changes in the Company's activities, changes in the legislation of the Republic of Kazakhstan and as necessary.

26. Issues not provided for in the provisions of this Policy are resolved in accordance with the legislation of the Republic of Kazakhstan, internal documents of the Company (at the same time, the legislation of the Republic of Kazakhstan has prevailing force).

27. Failure to comply with the procedure and rules for the use of information resources and the measures taken in the Company for the PDP entails liability in accordance with the current legislation of the Republic of Kazakhstan.

28. This Policy comes into force from the moment of its approval and is valid until the adoption of a new Policy.

29. The responsibility for making changes to this Policy is borne by the head of the SD IS.

30. Control over familiarization with this Policy is assigned to the head of the SD IS.

The list of personal data necessary and sufficient to perform the tasks performed:

№	The name of the task, including functions, powers, responsibilities	Purposes of collection and processing within the framework of the task being carried out	Name of personal data for a specific purpose	An indication of documents or regulatory legal acts that have direct indications of the tasks performed by the owner and/or operator