**Appendix to the Decision of the Board of Kazakhtelecom JSC No._____dated _____ 2026**

# Personal Data Protection Policy at Kazakhtelecom JSC

Almaty, 2026

## Content

## Chapter 1. General provisions

1. The Personal Data Protection Policy at Kazakhtelecom JSC (hereinafter – the Policy) has been developed in accordance with Subparagraph 1-1) of paragraph 2 of Article 25 of the Law of the Republic of Kazakhstan "On Personal Data and their Protection" (hereinafter – the Law), in order to define the basic principles of collection, processing and personal data of customers, suppliers, business partners, employees, and others, as well as defines the main actions for collecting, processing, and PDP in the Company.

2. The Policy is a fundamental document in the field of PDP, sets goals, objectives and principles in the field of PDP, which are guided by the Company in its activities, and serves as a guide in the development of relevant PDP documents.

3. The regulatory framework of the Policy consists of the Law of the Republic of Kazakhstan "On Informatization", the Law, subordinate regulatory legal acts adopted on its basis, as well as IRD (internal regulatory documentation).

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

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

## Chapter 2. Terms, abbreviations, and definitions

1. The Policy uses the following terms, abbreviations and definitions:

1) blocking – actions to temporarily stop the collection, use, distribution, depersonalization, destruction, as well as accumulation, modification, and addition of personal data;

2) PD protection (hereinafter referred to as PDP) – a set of organizational and technical measures aimed at protecting PD;

3) IS – information security;

4) information – information (messages, data) regardless of the form of their presentation;

5) use – actions (operations) with PD performed by an employee of the Company aimed at achieving the goals of the Company's activities;

6) PD confidentiality – the obligation to prevent persons who have gained access to PD from distributing them without the consent of the Subject or other legitimate grounds;

7) IRD – regulatory documentation of the Company (policies, standards, orders, regulations, manuals, instructions, etc.);

8) depersonalization — actions, as a result of which it is impossible to determine whether a PD belongs to a Subject;

9) processing — actions (operations) with PD aimed at their systematization, accumulation, storage, clarification (updating, modification), use, distribution (including transfer), depersonalization, blocking, destruction;

10) publicly available personal data – personal data that, in accordance with the laws of the Republic of Kazakhstan, are not subject to confidentiality requirements, access to which is free with the consent of the Subject;

11) Company – Kazakhtelecom JSC;

12) PD List – List of PD that is necessary and sufficient for the Company to perform its tasks;

13) personal data (hereinafter referred to as PD) – information processed by the Company or planned to be processed by the Company, related to a specific or determined Subject based on them, recorded on electronic, paper and (or) other material media;

14) dissemination — actions that result in the transmission of PD, including through mass media, or the provision of access to PD in any other way;

15) collection - actions aimed at obtaining personal data;

16) SD – structural division – a dedicated unit in the Company's structure (branch, department, center, service, department, etc.);

17) SIB – Information Security Service of the Central Office of the Company;

18) Subject – an individual to whom personal data relate;

19) cross-border transfer - transfer of PD to the territory of foreign states;

20) destruction — actions, as a result of which it is impossible to restore the PD.

21) the authorized body in the field of personal data protection (hereinafter referred to as the authorized body) is the central executive body responsible for managing PDP in the Republic of Kazakhstan.

Other terms, abbreviations, and definitions in the Policy have the meaning established for them by law, taking into account their application to PD.

## Chapter 3. Main goals and objectives

7. The main objectives, which are aimed at achieving all the provisions of the Policy, are:

1) continuity of PD availability to support the Company's business processes;

2) the integrity of the PD in order to support the high quality of the Company's business processes;

3) confidentiality of PD;

4) compliance of the measures taken under 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.

8. The main objectives for the implementation of the Policy are planning, implementing and monitoring the implementation of a set of organizational and technical measures to ensure the protection of personal data based on an assessment of the Company's risks in the field of information security, aimed at ensuring:

1) protection of personal data 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 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) the 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) awareness of employees about the Policy, measures taken, requirements for ensuring the PDP, duties and rules of conduct imposed on employees of the Company, as well as ensuring control over their proper implementation;

9) increase the level of knowledge and development of corporate culture in the field of personal data;

10) improving the PDP;

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

9. In order to achieve the specified goals and solve the listed tasks, the Company builds a PDP that meets the requirements:

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

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

10. The PDP, being part of the general management system of the Company, is documented in the 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 the Policy and binding on all employees of the Company, as well as third parties, representatives of third parties who have access to PD.

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

11. Procedure for obtaining (collecting) PD:

1) except in cases provided for by Law, collection and (or) processing is carried out after obtaining the consent of the Subject or his legal representative for collection and processing, including using information systems and for cross-border transfer, including to states that do not provide personal data (hereinafter referred to as Consent). Consent can be provided in writing, through a government or non-government service, or in any other way that allows you to confirm that you have received Consent (hereinafter referred to as the Established Method).;

2) The Consent is stored in paper or (and) electronic form in the personal file of the Subject;

3) The Consent is valid for the entire duration of the contractual and non-contractual relations of the Subject with the Company;

12. Consent includes:

1) the name and business identification number of the Company or operator, if the Company is not one of them;

2) last name, first name, patronymic (if it is indicated in the identity document) of the Subject;

3) the term or period during which the Consent is valid;

4) information about the Company's ability or lack thereof to transfer PD to third parties;

5) information on the presence or absence of a cross-border transfer during processing;

6) information about distribution in publicly available sources;

7) the list of collected data related to the Subject;

8) information on the possibility of cross-border transfer to States that do not provide a CPA;

9) other information determined by the Company, including its internal documents.

13. Processing without Consent is carried out in the following cases:

1) PD's are publicly available PD's;

2) at the request of authorized state bodies in cases stipulated by the legislation of the Republic of Kazakhstan.;

3) the processing is carried out for statistical purposes, subject to mandatory depersonalization.;

4) in other cases stipulated by Law.

14. Processing procedure:

1) the first head of the Company or a branch of the Company, as well as the person acting as the corresponding first head, depending on where the collection and processing is carried out, approves the list of persons who collect and process or have access to PD, and also appoints the person(s) responsible for organizing the processing;

2) The Subject provides the employee of the Company responsible for conducting operational work with information about himself;

3) based on the information received, an employee of the Company verifies the presence of this Subject in the Company's information system. If the Subject is not present in the Company's information system, the operational officer enters the necessary information about the Subject, after obtaining Consent in the Prescribed manner. If information about the Subject is available in the Company's information system, it checks the data with the previously provided ones (if necessary, makes appropriate changes).;

4) processing may be carried out solely for the purposes of collection specified in the List of PD;

5) the volume and content of processed PD should be minimally sufficient to achieve the purposes of collection and processing.

6) The list of PD is approved in a manner similar to the procedure established in subparagraph 1) of paragraph 14 of the Policy, after consultation with the SIB, in accordance with the annex to the Policy;

7) it is prohibited to collect and process copies of documents certifying the identity of the Subject on paper;

8) PD is processed in information systems, as well as on paper in the Company.

15. PDP:

1) A PDP is understood as a set of measures (organizational, administrative, technical) aimed at preventing unlawful or accidental access to PD, illegal destruction, modification, blocking, distribution, as well as preventing other illegal actions in relation to PD by persons who do not have access to PD;

2) The Company, in accordance with the legislation of the Republic of Kazakhstan, takes all necessary organizational, administrative and technical measures under the PDP, including encryption (cryptographic) tools, antivirus protection, vulnerability analysis, access control, registration and accounting, organization of regulatory and methodological measures regulating the PDP.

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

### §1. Blocking of personal data

16. The procedure for blocking and unblocking PD:

1) blocking is carried out within one business day after receiving a written application, other request from the Subject or his legal representative submitted through a state or non-state service, as well as in any other way that allows confirming the identity of the Subject or his legal representative, violation of the conditions of collection and (or) processing, as well as within one business day after self-determination of the fact of violation of the conditions of collection and (or) processing;

2) blocking means the temporary cessation of collection, use, depersonalization, destruction, distribution, as well as accumulation, modification, addition and editing of PD by any means (e-mail, cellular communication, information media, etc.);

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

4) the Subject's PD is unblocked within one business day after receiving a written application, other request from the Subject or his legal representative submitted through a state or non-state service, as well as in any other way that allows confirming the identity of the Subject or his legal representative, that there is no violation of the conditions of collection and (or) processing, as well as within one working day after non-confirmation of a violation of the conditions of collection and (or) processing;

5) obtaining repeated Consent to the processing of the Subject's data entails the unblocking of his PD.

### §2. Depersonalization and/or destruction of personal data

17. Depersonalization and (or) destruction are carried out on the basis of a decision of the commission on depersonalization and destruction (hereinafter referred to as the Commission). The Commission is formed in a manner similar to that

established in subparagraph 1) of paragraph 14 of the Policy and should consist of the chairman of the Commission, an employee responsible for organizing processing, and employees of the joint venture with access to PD, in the number of at least 3 people. The Commission draws up an appropriate act, which is subsequently kept by the Chairman of the Commission in a separate folder. Depersonalization occurs for conducting statistical, sociological, scientific, and marketing research:

1) when depersonalizing PD in information systems, they are replaced by a set of symbols that make it impossible to determine whether PD belongs to a specific Subject;

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

3) during depersonalization, paper media of documents are also destroyed with the preparation of an appropriate act, which is subsequently stored by the Chairman of the Commission in a separate folder;

4) the depersonalization and destruction operation is irreversible and cannot be restored.

## Chapter 6. Dissemination and storage of personal data

18. Dissemination means the transmission of PD through communication channels, on tangible media, orally, through mass media, providing access to PD, etc.;

19. When distributing, the Company's employees must comply with the following requirements:

1) strive to disseminate information within the Company among its employees;

2) distribute it in accordance with IRD's Policy and its own job descriptions;

3) access to PD is provided only to those employees of the Company who have the appropriate level and volume of access and for whom such data is necessary for the performance of official duties.;

4) the transfer of PD to third parties and cross-border transfer is carried out only with the consent of the Subject;

5) 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 IRD and limit this information only to those PD of the Subject that are necessary for the performance of their functions by these representatives.

20. PD storage:

1) PD storage means the existence of records in information systems and on material media of the Company, in respect of which the Company ensures integrity, confidentiality and accessibility;

2) PD is 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

information protection tools with parameters not lower than the third security level in accordance with the legislation of the Republic of Kazakhstan;

4) PD is stored in a database located on the territory of the Republic of Kazakhstan.

5) PD storage is carried out during the validity period of the Consent. The storage period of PD may exceed the validity period of Consent, if this is established by the laws of the Republic of Kazakhstan or an agreement with the Subject.

## Chapter 7. Access to personal data

21. Access to PD is provided to the Company's employees according to the approved list of persons who collect and process or have access to PD.

22. Access to PD contained in the Company's electronic information resources is provided to an employee of the Company in accordance with IRD, taking into account the Policy.

23. An employee of the Company is granted access to personal data if such access is necessary for the employee to perform his official duties in accordance with his job description, orders, and instructions from supervisors. In this case, the specified instructions must be recorded in writing.

24. Access to PD to other persons who are not employees of the Company is provided if such access is necessary for the implementation of agreements/contracts to which the Company is a party.

25. Access to PD is provided only to the following third parties (collectively):

1) access to personal data that is reasonably necessary for the implementation of these agreements/contracts;

2) informed about the confidential nature of PD;

3) having obligations to the Company not to disclose personal data on terms that ensure the safety of personal data. These obligations must be valid for the entire time that the PD is in the possession of such third parties.

26. Disclosure, transfer or provision of access to the received PD by the specified third parties to other third parties is not allowed.

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

27. The Policy is based on the following basic principles:

1) respect for the constitutional rights and freedoms of man and citizen;

2) legality of the provision of the PDP;

3) confidentiality of restricted access PD;

4) the involvement of the Company's management in the process of ensuring the PDP;

5) business orientation;

6) the process approach;

7) comprehensive use of methods, methods and means of protection;

8) following best practices;
9) reasonable sufficiency;
10) awareness and personal responsibility.

## Chapter 9. Roles and Responsibilities

28. Control over the implementation of the Policy requirements is assigned to the Managing Director for Information Security.

29. All interested joint ventures are responsible for ensuring proper compliance with the requirements of the Policy and the documents adopted on its basis.

30. Joint venture managers are responsible for timely communicating the Policy requirements to employees of their divisions and/or representatives of third parties as far as they are concerned, and for employees of their divisions and/or representatives of third parties meeting the Policy requirements.

31. All users should be familiar with the requirements of the Policy.

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

33. In the event of violations of the Policy requirements that have resulted in unauthorized access by unauthorized persons during the collection, processing or storage of PD, an internal investigation should be initiated and conducted with the involvement of interested joint ventures, as well as representatives of the authorized body.

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

## Chapter 10. Final provisions

35. The provisions of the Policy are subject to review once every five years, either based on the results of an external audit, internal analysis and assessment of information security risks for the Company's information system, changes in the legislation of the Republic of Kazakhstan, as a result of any changes in the Company's activities that significantly affect the procedure for collecting, processing and reporting data established by the Policy.

36. The head of the ISD is responsible for making changes to the Policy, as well as its relevance.

37. Issues not provided for in the Policy provisions are resolved in accordance with the legislation of the Republic of Kazakhstan, IRD (with the legislation of the Republic of Kazakhstan prevailing).

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

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

40. Control over familiarization with the Policy is assigned to the head of the ISD.

Appendix to the Personal Data Protection Policy of Kazakhtelecom JSC

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

| No. | Name of the task, including functions, powers, and responsibilities | Purposes of collection and processing within the framework of the task being performed | Name of personal data for a specific purpose | An indication of documents or regulatory legal acts that have direct references to the tasks performed by the owner and/or operator |
|---|---|---|---|---|
| | | | | |