

4.4.4. Markets and competition

4.4.4.1. Management approach

GRI 3-3

The approach to the management of anti-competitive behaviour at the Company includes a combination of legal, ethical and strategic measures. One of the fundamental legislative acts of the Republic of Kazakhstan by which Kazakhtelecom JSC is guided is the Law “On natural monopolies”.

The Company is included in the republican section of the State register of subjects of natural monopolies and performs the functions of an operator of “universal services”, in connection with which its activities are subject to regulation from the state.

The activities of Kazakhtelecom JSC in the sphere of tariff regulation and compliance with legislation on natural monopolies are carried out under the control of the Agency for Protection and Development

of Competition of the Republic of Kazakhstan as the authorised body in the sphere of regulation of natural monopolies and protection of competition. The powers in the sphere of antimonopoly regulation and protection of competition in respect of the Company are also exercised by the Agency for Protection and Development of Competition of the Republic of Kazakhstan.

Sectoral regulation of activities in the sphere of communications, including licensing, distribution of radio frequency spectrum and technical supervision, is carried out by the Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan through the Committee of Telecommunications. Issues of cyber and information security are supervised by the Committee of Information Security at the ministry.

GRI 2-27, GRI 206-1

For the reporting period, no cases related to violation of antimonopoly legislation and other legal actions in respect of the Company in connection with hindrance of competition have been registered at the Company.

Table 76. Cases of violations of antimonopoly and competition legislation in 2025, pcs. A

Area of focus	2025
Total number of confirmed cases of anticompetitive behaviour	0
Total number of violations of antimonopoly and competition legislation	0

4.4.5. Information security and data protection

According to the results of the materiality analysis disclosed in section “Materiality analysis” , information security and data protection have been recognized as one of the material topics of Kazakhtelecom JSC. Upon the determination of materiality, the Company took into account the expectations of stakeholders, the results of questioning, internal expertise, and also the impact of the topic on the resilience of digital infrastructure, the quality of services, the trust of clients, regulatory compliance and long-term value creation.

For Kazakhtelecom JSC, this topic is of material significance with account for the role of the Company as a national communications operator, the scales of processing of client and corporate data, the development of digital services, AI solutions, data centres and network infrastructure. An insufficient level of information security may lead to the disruption of continuity of services, data leakage, regulatory consequences, reputational losses and the reduction of trust of clients, partners and state bodies. Therefore, the Company regards information security and data protection as one of the key factors of sustainability of business and long-term value creation.

4.4.5.1. Management approach

GRI 3-3, 418-1

The Information Security Service is in direct subordination to the Managing Director for Information Security, to whom the Head of the Information Security Service is accountable, which ensures the control of issues of information security at the strategic and operational levels.

Issues of the functioning of the information security system are submitted for consideration of the Audit

and Sustainability Committee under the Board of Directors. The Committee considers key issues related to the management of information security risks, the protection of personal data, the results of monitoring and inspections, the fulfilment of measures on the development of the information security system, as well as compliance with the requirements of legislation and IRDs of the Company. The consideration of these issues at the level of the Committee strengthens the supervision from the Board of Directors and makes it possible to take into account information security risks in the making of management decisions. Reporting on key risks, incidents in the sphere of IS and the implementation of measures is submitted to the Audit and Sustainability Committee on a regular basis in accordance with the internal procedures of the Company.

The main internal documents regulating issues in the area of information security are:

- Information Security Policy.
- Policy on the protection of personal data at Kazakhtelecom JSC.
- Concept on information security.

The documents of the Company regulating issues in the area of information security can be reviewed on the company’s website in the “Sustainable development” section, the “Information security and data protection” subsection.

Main principles of ensuring information security:

- fulfilment of legislative norms;
- involvement of senior management of the Company in the process of ensuring IS;
- orientation to business;
- process approach;
- integrated use of organizational and technical protection measures;

- following best practices;
- reasonable sufficiency;
- awareness and personal responsibility.

For ensuring information security, Kazakhtelecom JSC applies a systemic approach. One of the important aspects is round-the-clock control of data at all stages of their life cycle, starting from the moment of their entry into the Company's infrastructure and ending with their archiving or irreversible destruction.

At the Company, international practices of ensuring information security are applied. Our internal systems are protected with the help of such solutions as secure remote access to information resources, secure use of the internet, control of privileged users (PAM), vulnerability scanners, database protection and others. The Company strives to counter both external and internal threats and introduces new solutions and methods of work with resources, including the creation of the necessary infrastructure at the Company, the training of qualified specialists, the formation of the information security operations centre and the introduction of the ZeroTrust concept.

Also at the Company, such important security elements are used as integration into the state cybersecurity system EShDI, security of the Internet of things, the use of Honeypot traps and Machine Learning technology. In addition, on a permanent basis, training and the enhancement of IS awareness of the Company's employees is conducted. The Corporate University programme provides for a course familiarising employees with the Information Security Policy of Kazakhtelecom JSC, developed with the aim of determining strategic goals, tasks and main requirements for the complex of measures in the area of information security. These measures make it possible to support the culture of responsible handling of information and to minimise the risks of the human factor.

At the Company, a certificate of compliance with the standard ISO 20000-1 "Service management system" is in effect, which confirms the presence of processes of management of IT services, including requirements for reliability, continuity and security of services provided.

In October 2025 (28–29 October), an inspection audit of the Corporate Business Division (branch of the city of Almaty) was conducted on compliance with the requirements of the standard ST RK ISO/IEC 27001-2023 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements". Based on the results of the audit conducted by Kazakhstan Quality Centre LLP, compliance of the information security management system with the established requirements was confirmed.

On 31 October 2025, the Certificate of compliance with the standard ST RK ISO/IEC 27001-2023 was issued.

Plans for 2026:

Completion of introduction and passing of certification of the information security management system in the branch of the Information Technologies Division with the receipt of the certificate of compliance with the standard ISO/IEC 27001 (planned period — March 2026).

4.4.5.2. Protection of personal data

GRI 418-1

At the Company, the "Personal Data Protection Policy" has been developed and introduced, approved by order of the Chairman of the Management Board of the Company of 06.10.2023 No. 313, in which the main principles of processing of personal data of clients, suppliers, business partners, employees and other persons are determined, and also the main actions for the collection, storage and processing of personal data, as well as measures on their protection, are determined.

On the basis of the Law of the Republic of Kazakhstan of 17 November 2025 No. 231-VIII "On the introduction of changes and additions to certain legislative acts of the Republic of Kazakhstan on the issues of artificial intelligence and digitalization", changes were introduced into the Law of the Republic of Kazakhstan "On personal data and their protection". In this connection, changes were introduced into the Policy in the following directions:

- updating of the list of terms, abbreviations and definitions;
- improvement of the process of obtaining consents to the collection and processing of personal data;
- unification of approaches to the order of obtaining consents to the collection and processing of personal data;
- introduction of the order of approval of the list of persons carrying out the collection and processing of personal data or having access to them, as well as the appointment of a person (persons) responsible for the organization of processing of personal data;
- improvement of the processes of blocking and storage of personal data;
- correction of the processes of provision of access to personal data.

The Policy is a fundamental document in the area of personal data protection, establishes the goals, tasks and principles in the area of PD protection, by which the Company is guided in its activities. It serves as a guide upon the development of corresponding documents of personal data protection.

Main principles of ensuring the protection of personal data:

- observance of constitutional rights and freedoms of a human and a citizen;
- legality of ensuring the protection of personal data;
- confidentiality of personal data of restricted access;
- involvement of the Company's management in the process of ensuring the protection of personal data;
- orientation to business;
- process approach;
- integrated use of methods, methods and means of protection;
- following best practices;
- reasonable sufficiency;
- awareness and personal responsibility.

For the assessment of the effectiveness of the implementation of these principles and the control of risks of violation of confidentiality, the metric "Number of incidents that led to the leakage of personal data of subscribers of the Company" is applied. This indicator is directly related to the right of subscribers to confidentiality and the protection of personal information. This indicator reflects the interests of external stakeholders and demonstrates the Company's aspiration to ensure a high level of information security.

This metric is part of the risk management system and is included in the Key Performance Indicators (KPIs) of the General Director of the Information Technologies Department. For it, a target benchmark has been established — 0% of incidents, which corresponds to the policy of zero tolerance to leakages of personal data.

In addition to this, in the KPI system of the General Director of the Information Technologies Department, other indicators are used, reflecting the Company’s approach to the management of risks in the area of information security and the client experience, including:

- Client loyalty index (Net Promoter Score, NPS);
- Implementation of measures on the additional equipping of the ZeroTrust core;
- Share of timely eliminated information security incidents;

4.4.5.3. Main results for the reporting period

In the area of information security, in 2025 at the Company a complex of measures was conducted to ensure the protection of corporate information systems, personal data, official information and data transmission networks.

Information security employees, on a regular basis, conduct exercises on the actions of users upon the receipt of suspicious letters. The work of the Information Security Operations Centre (ISOC) with a 24/7 functioning mode is constantly being improved. The main duties include:

- Protection of the corporate perimeter of the Company;
- Monitoring of information security (IS) events;
- Response to IS incidents;
- Investigation of IS incidents;
- Search for vulnerabilities in the information systems of the Company;
- Issuance of recommendations on the elimination of information security incidents;
- Control of information protection means (IPMs).

- Other metrics aimed at the protection of the interests of users and the strengthening of trust in the Company’s digital services.

Monitoring and control of the indicated indicators are carried out constantly within the framework of the Company’s internal regulations on information security.

In May 2025, the Committee of Information Security of the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan conducted a verification of compliance with the requirements of legislation in the sphere of information security. Based on the results of the verification, no violations in respect of the protection of personal data were identified.

In 2025, the third stage of the transition of the Company to the ZeroTrust model was implemented, the introduction of a number of software and hardware information protection means (IPMs) was carried out, which made it possible to strengthen the existing protection of the corporate infrastructure of the Company.

The total number of substantiated complaints received in respect of violation of the confidentiality of clients is equal to zero. Including:

- Complaints received from third-party persons and substantiated organizations — 0;
- Complaints received from controlling bodies — 0;
- Identified leaks, thefts or losses of client data — 0.

These indicators are evidence of the absence of registered incidents related to the violation of the confidentiality of clients for the reporting period.

Results of the work of the corporate ISOC:

About **9,000** DDoS attacks on clients’ resources were repelled (peak value more than 400 Gbit/sec), with total traffic more than 1,230 Tbit.

About **80 traps** (Honeypot — fully imitating information systems/ resources of the company) were deployed, which made it possible to identify more than **50,408 malicious requests** inside the corporate network of the company.

The antivirus solution identified about **260,000 cases** of detection of malicious activity and suspicious objects.

By scanning vulnerabilities of web applications and software, about **60.9 thousand active vulnerabilities** were identified on 98.8 thousand of the Company’s assets; more than 55.6 thousand vulnerabilities were eliminated by responsible administrators (61.66% of the total number).

Within the framework of the functioning of the SIEM system, centralized reception and correlation of data from **567 log sources** is carried out, which made it possible to identify and process more than **4,873 critical** and high-risk events inside the corporate network of the company.

With the help of WAF, about **27.3 million web requests** to Internet resources were registered. Of which 1.75 million malicious attempts were successfully repelled.

With the help of the privileged users control system PAM, more than **305 privileged users** (administrators of information systems, external users and contractors) have access to more than 420 IP addresses of terminal servers of corporate information systems.

The DLP system registered about **1.5 million events**. The main activity fell on the USB, File Share and Clipboard channels.

Jointly with the Department on counteraction of fraud (FROD), work is being conducted on the identification of sources of fraud traffic located abroad; more than **7 million fraudulent calls were blocked**.

4.4.5.4. Informing and training of employees on issues of information security

GRI 418-1

At the Company, a systemic programme of enhancement of awareness of employees in the area of information security is being implemented, aimed at ensuring confidentiality, integrity and accessibility of data.

Information materials on issues of information security are regularly sent to employees through the electronic document management system. All organizational and administrative documents of the Company, including documents in the area of information security, are brought to the attention of employees by the Quality Group with the obligatory fixation of the fact of familiarisation.

Training trainings on issues of information security and protection of personal data are conducted with subsequent testing for the verification of the level of understanding and assimilation of requirements. In the reporting year, the Information Technologies Department (ITD) initiated an additional format of training of employees with the use of presentation materials and practice-oriented cases aimed at the analysis of standard incidents and the formation of skills of safe behaviour upon work with information resources. With the aim of assessing resistance to social engineering attacks, phishing exercises are organized: employees are sent simulated phishing letters with attachments, facts of opening of letters, attachments and filling out of forms are registered, and the results are used for conducting additional explanatory work.

Information security is ensured both at the administrative level — every employee is obliged to familiarise himself with and fulfil the requirements of regulations, rules, policies of the Company in the area of information security, and at the technical and physical level — at the company, various hardware and software complexes, means of cryptographic protection of information, etc., are used.

In addition, specialists of the IS Division regularly undergo various courses of enhancement of qualifications on information security, cybersecurity, IS risks and threats. For employees of subdivisions on work with clients and on work with personnel, where the risk of unlawful use of data is sufficiently high, general training/testing on improving cyber hygiene is conducted.

Table 77. Indicators on the material topic affecting the long-term value creation of the Company

Indicator	Target for 2025	Result 2025
Number of incidents that resulted in the leakage of subscribers' personal data	0 incidents	0 incidents ^A
Share of information security incidents resolved on time	100%	100%
Identification and elimination of vulnerabilities	Timely elimination of critical and high-risk vulnerabilities	60.9 thousand vulnerabilities, identified 55.6 thousand eliminated
Data protection and counteraction to fraud traffic	Detection and blocking of fraudulent traffic	about 9,000 DDoS attacks repelled more than 1,230 Tbit of DDoS traffic more than 7 million fraudulent calls blocked

Indicators in the area of information security and data protection, including the metrics “Number of incidents that led to the leakage of personal data of subscribers of the Company” and “Share of timely eliminated IS incidents”, are included in the KPIs of the Managing Director for Information Security and the Head of the Information Security Service. The fulfilment of KPIs is taken into account in the variable part of their remuneration in the order established by the internal documents of the Company.