MARKETS AND COMPETITION

MANAGEMENT APPROACH

GRI 3-3

The management of anti-competitive behavior at Kazakhtelecom JSC involves a combination of legal, ethical, and strategic measures. One of the fundamental legislative acts followed by the Company is the Law of the Republic of Kazakhstan "On Natural Monopolies."

The Company is included in the national section of the State Register of Entities of Natural Monopolies and performs the functions of a "universal service" operator, which subjects its activities to state regulation.

The antimonopoly regulation of Kazakhtelecom JSC's activities is overseen by the authorized body for natural monopolies in the telecommunications sector – the Committee for State Control in the Sphere of Communications, Informatization and Mass Media under the Ministry of Information and Communications of the Republic of Kazakhstan. The authority for competition protection with respect to Kazakhtelecom JSC is exercised by the Committee for Regulation of Natural Monopolies, Protection of Competition and Consumer Rights under the Ministry of National Economy of the Republic of Kazakhstan.

GRI 2-27, 206-1

During the reporting period, the Company did not record any cases related to violations of antimonopoly legislation or other legal actions against the Company in connection with obstruction of competition.

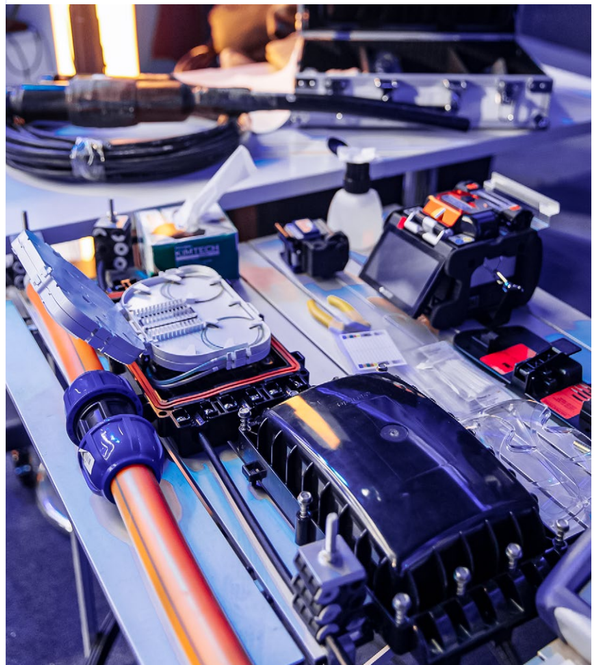
INNOVATION AND NEW TECHNOLOGIES

MANAGEMENT APPROACH

Innovative technologies play an important role in achieving the strategic goals of the Company and contribute to the creation of high-quality and user-friendly services for millions of people in Kazakhstan.

The implementation of innovative projects and the digital transformation of the Company help enhance management efficiency, minimize risks, and support alignment with ESG principles and the achievement of the UN Sustainable Development Goals.

Kazakhtelecom JSC develops and implements various digital products and solutions for individuals, businesses, and the public sector.



NEW BUSINESSES AND NEW PRODUCTS

DDoS Attack Protection

DDoS attack protection is one of the most in-demand services among corporate clients in Kazakhstan.

The "DDoS Attack Protection" service comprises a set of measures aimed at providing maximum resistance to and prevention of DDoS attacks from the Internet, based on solutions from global leaders in the field of cybersecurity. The service helps reduce risks related to the unavailability of public resources due to bandwidth saturation or critical equipment overload caused by DDoS attacks.

As part of the "Establishment of a SOC and Information Security Services for B2B/B2G" project, two additional AntiDDoS scrubbing devices were deployed in Astana using the INLINE scheme. These devices provide protection against internal DDoS attacks for Kazakhtelecom JSC subscribers. Preparations for their commissioning and the development of a product catalog for the service are currently underway.

In Almaty and Astana, a hardware and software complex for "Intrusion Protection" has been deployed, which includes a Next Generation Firewall, Web Application Firewall, Email Protection, and Sandbox. At present, pilot sales of the "Firewall Service" are being conducted.

Internet access with cache server integration

Cache servers are part of the infrastructure of the largest content providers – online games, video hosting platforms, streaming services, and social networks – hosted in Kazakhtelecom JSC's data centers within Kazakhstan. The product offered by Kazakhtelecom provides Internet access and access to the Company's cached resources for subscribers in the B2O segment.

Using this product allows clients and end users to significantly reduce the time needed to access popular resources. It also helps lower costs associated with the purchase and maintenance of expensive equipment such as data storage systems, servers, power supply units, and network infrastructure.

TELECOMMUNICATIONS INFRASTRUCTURE AND NETWORK DEVELOPMENT

Modernization of Backbone Data Transmission Network (BDTN)

In 2024, the implementation of the project "Expansion of Port Capacity for Operator Connections" was completed. During the 2020–2024 period, the following measures were carried out:

- Expansion/installation of ASBR (Autonomous System Border Routers) of the backbone data transmission network;
- Expansion of external Internet channels on ASBR routers of the backbone data transmission network;
- Expansion of port capacity on MX-PE routers of the backbone data transmission network;
- Expansion of port capacity on MASG routers of the Mobile Backhaul network;
- Expansion/modernization of core P-routers (PTX) of the backbone data transmission network;
- Expansion/installation of DWDM backbone channels;
- Expansion/installation of SpeedTest servers to monitor the quality of data transmission services across the backbone data transmission network.

In 2024, service edge routers were upgraded. As a result of installation and commissioning works, telecommunications operators can now connect to 100 Gbps ports in the cities of Astana, Almaty, Aktobe, Shymkent, Karaganda, Atyrau, Taraz, Pavlodar, Kyzylorda, Semey, Uralsk, Kostanay, Aktau, and Ust-Kamenogorsk.

Expansion of Network Infrastructure (Peering) and Caching Servers to Optimize Content Access

In 2024, new caching servers were launched for VK, CloudFlare, Baishan, Microsoft, and others. The total volume of localized traffic throughput exceeded 5 Tbps. A cluster of high-performance servers was deployed in Pavlodar to support the launch of various services.

Significant investments were made in the data center in Astana to improve power supply, cooling systems, data transmission equipment, racks, and other infrastructure components. These improvements will enable the hosting of a substantial number of caching servers in the coming years.

In 2024, successful negotiations were held with Telegram, resulting in the establishment of a direct peering connection at one of the Company's points of presence (POP) with a total capacity of 100G. A commercial contract was also successfully implemented with MTS for access to Telegram peering.

DNS Service Improvement

In cooperation with ISC and Netnod, root DNS servers F.ROOT and I.ROOT were commissioned on the Company's data network in Pavlodar. This significantly enhances DNS reliability, reduces latency, and improves network security for millions of users in the region. The development of DNS infrastructure contributes to the resilience of the global Internet system by providing more stable connectivity for users in Central Asia.

This project is part of Kazakhtelecom JSC's broader effort to strengthen the region's digital infrastructure. The local deployment of additional root DNS servers accelerates query processing and reduces DNS response times.

5G Project

In 2024, Tele2 and Kcell successfully deployed 5G base stations in 20 cities across the Republic of Kazakhstan, fully meeting and even exceeding their licensing obligations to the government. In addition, Kazakhtelecom successfully implemented its plans to build a 5G MBH (Mobile Backhaul) network for mobile operators.

The total cost of the project amounted to KZT 536.9 billion.

Construction of a Submarine FOCL across the Caspian Sea project

The following activities were carried out under the project in 2024:

- As part of the "Construction of the FOCL along the bottom of the Caspian Sea" project, in 2024 the joint venture Caspinet B.V. (50% – Kazakhtelecom JSC, 50% – Azertelecom Int. LLC) prepared tender documentation and held a tender to select an EPC contractor for the design and construction of the submarine FOCL along the Caspian Sea, as well as a contractor for supervision services. Following the tender process, a contract was signed with a qualified EPC contractor for the design and construction of the submarine FOCL along the route from Aktau (Kazakhstan) to Sumgait (Azerbaijan). A separate contract was also signed with a company responsible for technical supervision of the works.
- Simultaneously, preparations began for the construction of the required onshore infrastructure. Design and construction works are underway for the beach manhole and cable landing stations in the city of Aktau. These facilities will serve as key nodes for integrating the submarine cable into the terrestrial networks.
- At present, the project is in the active preparatory phase for marine operations, including seabed surveys and route planning.

The total project cost amounted to KZT 23.0 billion.

Development of Fixed Wireless Access (FWA) in Rural Areas

The subsidiary Auyl Telecom LLP is implementing pilot projects to develop fixed wireless access (FWA) in rural areas, providing high-speed internet in locations where the construction of fibre-optic communication lines (FOCL) or GPON networks is economically unfeasible. This initiative helps reduce the digital divide and deliver modern connectivity to residents of remote regions.

As part of the pilot projects, solutions based on Open RAN and 5G FWA have already been tested. In the village of Sarybay, the average connection speed increased 85-fold – from 5 Mbps to 427 Mbps – significantly improving the quality of online education, telemedicine, and remote work. Thus, FWA not only modernises outdated technologies (WiFi, ADSL, CDMA EVDO) but also becomes a key tool in bridging the digital gap between urban and rural areas.

Auyl Telecom continues to actively expand its FWA network, with 5G being a strategic focus for the company. However, a 4G network is also being developed in parallel. A successful example of implementation is the village of Karatala in the Aktobe region, where 79 out of 120 households have been connected. The average connection speed is 46 Mbps, and the average internet traffic consumption per household over a three-week period reached 191 GB. For 10 subscribers, the data usage exceeded 450 GB during the same period.

Testing of various network functions and technical solutions

- The technical feasibility and readiness of the hardware and software complex based on Open RAN 5G Fronthaul for providing Internet access via fixed wireless access were tested. The operability of the Open RAN 5G Fronthaul solution was confirmed with some limitations.
- The invGUARD AS-SW software suite was tested to evaluate its capabilities in monitoring and analyzing network traffic statistics on the Kazakhtelecom JSC network within the TelcoCloud environment.
- The VOLTHA GPON technology was tested in the TelcoCloud environment in the city of Konaev. The main idea of this solution is disaggregation and avoidance of vendor lock-in. In traditional GPON, OLT (stationary equipment), software, licenses, and ONT (customer premises equipment) are supplied by a single vendor and are “locked,” which prevents connecting ONTs from other manufacturers to an OLT of a different vendor or using software from other providers. The VOLTHA solution overcomes these restrictions by allowing the selection of white-box OLT hardware from one manufacturer, software and licenses from another, and using the openOMCI standard to connect ONTs from different vendors.
- The product is not yet fully ready, but the concept and implementation activity are already delivering results. The pilot broadband project based on VOLTHA is currently being implemented in Konaev.
- The service of providing access to cache servers for telecom operators in Kazakhstan and Central Asia was tested.
- Testing has begun on an indoor solution to provide mobile Internet access using PicoCell in locations with poor mobile/broadband signal quality (e.g., shops, cafes located in basements).

INFORMATION SECURITY AND DATA PROTECTION

The Company recognises the importance of ensuring information security and protecting its clients’ data. Kazakhtelecom JSC continues to develop a robust information security and data protection management system.

MANAGEMENT APPROACH

GRI 3-3, 418-1

The Information Security Service reports directly to the Managing Director for Information Security, who oversees information security issues at the highest level within the Company.

The key internal documents regulating information security include:

- Information Security Policy;
- Personal Data Protection Policy of Kazakhtelecom JSC;
- Information Security Concept.

These documents are available on the Company’s website in the “Sustainable Development” section, under the “Information Security and Data Protection” subsection.

Key principles of information security management:

- compliance with legal requirements;
- involvement of top management in the information security process;
- business orientation;
- process-based approach;
- comprehensive use of methods, tools, and means of protection;
- adherence to best practices;
- reasonable sufficiency;
- awareness and personal accountability.

To ensure information security, Kazakhtelecom JSC applies a systematic approach. One of the key aspects is round-the-clock monitoring of data throughout their entire lifecycle – from the moment they enter the Company’s infrastructure to their archiving or permanent deletion.

Currently, the Company applies globally recognized best practices in information security. Internal systems are protected using solutions such as secure remote access to information resources, safe internet usage, privileged access management (PAM), vulnerability scanners, and more. The Company strives to counter external threats and implements new solutions and methods for handling resources, including the development of internal infrastructure, training of qualified specialists, the establishment of a Security Operations Center (SOC), and the adoption of the Zero Trust concept.

Other important security components used by the Company include integration into the national cybersecurity system (YShDI), Internet of Things (IoT) security, deployment of honeypots, the use of machine learning, and other advanced technologies. In addition, regular training and awareness-raising activities are conducted to enhance employees’ knowledge of information security.