● Our performance: Safeguarded security and privacy

Security first and fostering privacy

We want everyone to enjoy the benefits of connectivity carefree, so we strive for security first at KPN. Security is one of our most material topics and we follow various security policies. By creating employee awareness, we are able to foster the right security and privacy mindset.

KPI	Result 2023	Result 2022
The percentage of Dutch population who believe their data is safe with KPN	61%	69%
SME KPN EEN customers that activates safe internet	62%	52%
Technical employees who are SecurX certified[1]	60%	N/a

[1] For definition, we refer to the glossary (Appendix 14)

Chapter contains information on material sustainability matters
- 02. Cybersecurity, data and information protection (entity specific)
- 15A. Privacy for company's consumers and end-users (ESRS S4)
- E. Security (entity specific)

Security first

Security organization

Protecting our customers, partners, and own operations against cyber risk is a top priority for KPN and one deeply engrained in our strategy. Under the umbrella of our 'Security First' program, we continuously work to assess and mitigate cybersecurity risks. These efforts are led by our Chief Information Security Office (CISO). In order to raise awareness on security and what everyone can do to keep KPN safe for our customers, all employees are supposed to do an e-learning on Cybersecurity every two years.

The scale and complexity of cyber attacks is growing globally. Ransomware, malicious phishing, and malware are increasing problems worldwide. Vital infrastructure such as our data network is considered an interesting target for state actors and other attackers. To respond to these threats and risks, our Chief Information Security Office is organized into four teams:
- The CISO Office sets a KPN security policy aimed at preventing vulnerabilities and incidents.
- The CISO REDteam, a team of ethical hackers, conducts security testing of new products and services and proactively identifies vulnerabilities across the organization.
- The BLUEteam, consisting of three subteams: First, Security Operations Center (SOC) that is responsible for monitoring our networks and infrastructures and reacting on security alerts in a timely manner. Second, KPN Computer Emergency Response Team (KPN-CERT) that provides incident response and forensic investigation. And third, the abuse desk that monitors the reputation of KPN on the internet and informs customers about network abuse issues.
- The CISO Monitoring & Reporting Team is responsible for security compliance monitoring and security analytics and reporting.

To further embed security awareness and preparedness in our organization, we launched our '4As'-strategy in 2023 as part of our Security First approach. The four As are: adaptive, automate, awareness and assure. 'Adaptive' means that we prepare ourselves as a company to be able to effectively respond to cyber threats and to improve this readiness. We wish to

Our performance: Safeguarded security and privacy

'automate' the protection of our assets as much as possible. This will ensure our security process runs smoothly and at the same time provides accurate insight into the level of security and protection at any given moment – creating real-time insight into all our assets. We want to continue efforts to enhance cybersecurity 'awareness' and make everyone at KPN conscious of the fact that the human factor is often crucial in protecting against cybersecurity risks – many threats are linked to potential human errors. We provide training and information about security to employees. 'Assure' refers to assuring that we act in line with our policy and comply with security regulations. To this end, we maintain a security compliance process.

We believe that, through this 4A-strategy and other existing initiatives, we strengthened our commitment to and management of cybersecurity. In addition, we significantly increased the size of the CISO team in 2023. This enables CISO to not only develop policies, but also monitor and supervise their implementation. We continued – and where possible intensified – our internal security awareness efforts, providing more information on our intranet and increasing the number of phishing email tests. In 2023, over 1,800 of our employees followed security training and we plan to provide security training to even more KPN staff to familiarize them with the basics of cybersecurity. CISO enhanced its focus on business unit level, as it is in business units that most security-related measures are implemented. In light of this, we created a new security platform to facilitate closer cooperation between CISO and KPN's business units (B2B, B2C, Wholesale, and TDO). We are on the brink of completing the implementation of measures required to comply with the Dutch government's Ministerial Decree regarding network security.

We continued so-called 'pentests' (or penetration testing), performed by our REDteam on new services and products before we launch them. Pentests allow us to take measures at an early stage in case we find security vulnerabilities. In addition, we executed several redteaming services exercises.

We measure our cybersecurity maturity against the NIST Cybersecurity Framework, an internationally recognized benchmark for our industry. An external assessment by advisory firm PWC in 2023 showed that KPN has been making progress in strengthening its cybersecurity governance and security capabilities in several categories compared to the previous assessment in 2021. The outcome of the assessment is input for our improvement plan and roadmap. Our ambition is to further improve our cybersecurity posture based on this plan and roadmap.

Security partners

KPN is a member of the Foundation NL CISO Circle of Trust (CCoT), together with nine other major companies, such as ASML, Philips, and AkzoNobel. The CCoT was set up to enhance collaboration and share knowledge and expertise between partners in the Netherlands. In 2023, CCoT acquired a license from the Dutch government (OKTT-status) enabling us to exchange cybersecurity information with partners and the government. We also created a platform to facilitate the exchange of information between CCoT partners. KPN plays a leading role in Dutch society in the field of cybersecurity. For example, KPN actively collaborates with the Dutch Government, scientific institutes and other private companies. KPN is member of the Anti-DDoS-Coalition. This coalition is a joint initiative to share knowledge and experiences in the field of DDoS attacks.

CHALLENGES

Implementing new security measures and protocols, such as shifting to automated ways to identify vulnerabilities quicker, and getting insight into the security status of our assets, can be a challenge at KPN. For instance, the speed at which we roll out two-factor-authorization across our operations needs to be kept in balance with the staff capacity required to realize other priorities, such as maintaining the stability of our networks. At the same time, we see opportunities to make our security approach more effective. We began exploring how we can shift to a risk-based way of working. This means shifting from an approach where staff involved need to comply with all relevant policies, to one where we can prioritize and fix the biggest threats first before addressing minor ones, so allocating our engineers and cybersecurity specialists more efficiently.

Security monitoring and incident response

In our first line of defense, our Security Operation Center (SOC) monitors our network 24/7, 365 days a year. We use AI to analyze billions of events and to gradually automate our monitoring. Last year, our security operations center (SOC) engineers analysed around 19,000 events. When there are grounds, KPN Computer Emergency Response Team (KPN-CERT) performs further in-depth investigations. We continuously train our security teams to maintain resilience against cybersecurity attacks.

Awards

KPN CISO once again participated in the annual Capture The Flag exercise organized by the Dutch Ministry of Defense and was a runner-up. During the international Hack in The Box, Capture The Flag, CISO REDteam (SectorC) came fifth.

New strategy

Security will be a core priority in our new business strategy and our Security First approach will maintain its central role. We have added our efforts to strengthen cybersecurity to our sustainability strategy and goals, as a secure internet is crucial to protecting privacy and enabling the safe use of our apps and services.

Our performance: Safeguarded security and privacy

Privacy

Digitalization and the ever-growing number of connected devices, bring more possibilities to society. But they also bring threats. The Dutch Data Protection Authority has reported that there were 21,151 data breach reports in the Netherlands in 2022. Numbers for 2023 have not been published yet. The importance of protecting customers' personal data therefore remains unchanged. Customers need to be able to trust that their data is safe with KPN. KPN has a Privacy Office to monitor and advise on data protection.

The Privacy Office consists of the Data Protection Officer (DPO) and two privacy advisors. They advise the business units on various privacy issues in close collaboration with privacy lawyers. They increase awareness through e-learning and specific training, such as for Young Talents within KPN. The latter is done together with the Compliance Office. In 2023, the DPO also participated in a panel discussion on the day of the DPO organized by the Dutch Data Protection Authority (AP) about the role and position of the DPO.

Every year we conduct a random survey in which we ask the Dutch population to name three companies where they think their data is the safest. In 2023, 61% of the Dutch population said they believe their information is safe with KPN (2022: 69%). Compared to last year, there is a decrease in the scores of all major telecom providers. On this score, KPN remains ahead of the competition in terms of the security and privacy of personal data in the eyes of the Dutch population.

New initiatives

After introducing two-factor authentication (2FA) last year for logging into the MijnKPN environment, KPN this year developed the option to log in to the website by scanning a QR code from the MijnKPN app. This makes it easy for customers to log in securely and secure their data.

In the second half of the year, KPN introduced two new services for consumers. A Password Manager (1Password) that ensures that passwords, credit card and login details can be managed securely by our customers. In addition, network security for customers' home networks. This means consumers can protect themselves better against, for example, malware, phishing, and unwanted content.

What do you think?

Share your opinion now on the statement below and 9 other thought-provoking topics that impact our company and environment.

Quality always comes first, even over cost

Scan and vote along!

Our performance: Safeguarded security and privacy

Privacy awareness

All employees must abide by the KPN Code of Conduct, which provides clear privacy guidance, including how to deal with customer information. They must also perform our privacy awareness e-learning training every two years. The rules regarding the use of employee data are laid down in the Human Resource Privacy Statement.

Our business is guided by the principle of ‘privacy by design’. This means we consider privacy and security risk from the earliest stage when developing new products and services. A pre-Data Protection Impact Assessment has been performed in the case of high-risk processing of personal data and the results are submitted to the Data Protection Officer for a decision.

In 2023, we received 423 notifications related to privacy, and reported 55 data leaks to the Dutch Data Protection Authority (AP) regarding customer data. Where necessary, we have informed customers about the leaks and the measures we have taken to stop them.

Artificial intelligence

At KPN we see the potential value of AI and apply this new technology within our processes. AI is changing the way we conduct our daily affairs. It brings new risks. And this is why we take measures to apply AI in a responsible and safe manner. Ethical considerations are part of the process – we are transparent about what we do with AI, who is responsible for the application and how we can intervene. We choose a proactive attitude when implementing measures and work together with universities in this dynamic field. We bundled this information in our KPN Responsible AI Framework.

Lawful intercept

We respect our customers’ right to privacy. At the same time, we are legally obliged to disclose certain information, obtained by intercept, to national investigation agencies. Our infrastructure must facilitate this, and we are obliged to cooperate with law-enforcement agencies as specified in the Dutch Telecommunications Act.

To help achieve this, a KPN liaison officer is available 24/7 to facilitate interaction with law-enforcement authorities for all KPN brands. We assess incoming warrants and carry out checks to filter out any uncertainties. If we find discrepancies, we reject the warrant, inform the agency involved, and follow the relevant procedures. In 2023, a mismatch was found in 1.2% of warrants received.

In the context of the Notice and Take Down Code of Conduct, KPN received 41 complaints in 2023. These complaints regarded copyright and intellectual property disputes. In none of the cases did KPN provide the identity information, as the criteria therefor were not met.