Data protection

We respect our users' right to privacy and protect their data. Our goal is to ensure data security of Kaspersky users.

~4,000
employees completed an internal course on working with user data

3,000+
requests for processing user data in 2023

GRI 418-1

Key objectives

- Ensure the data protection of all our users worldwide using the best information security practices and in compliance with local regulations.
- Promptly respond to privacy enquiries of our users regarding the processing and protection of their data.
- Prevent unauthorized access and risks to data processing.

GRI 3-3

Our approach to data protection

We are fully committed to protecting the data of our users worldwide. We protect our users' personal data[1] against possible unauthorized changes, compromise or loss. To this end, we use best-in-class technology and take the following security measures:

- The secure software development life cycle ensures the creation of secure products and the prompt correction of vulnerabilities.
- Reliable encryption ensures secure data exchanges between the user's device and the cloud.
- Digital certificates enable legitimate and secure server authentication and application updates.
- Data is stored separately on multiple servers with limited rights and strict access policies.
- Data is anonymized using various methods, including removing account data from transmitted URLs, obtaining the hashes of malicious files instead of the files themselves and hiding user IP addresses, etc.

[1] Personal data refers to any information relating to an individual, including his/her full name, telephone numbers, address, IP address or email address.

How we ensure data protection of our users worldwide

TC-SI-220-a.1 TC-SI-230-a.2

We are guided by the key data processing principles of the 2016 EU General Data Protection Regulation (GDPR). This legislative act prescribes the fundamental technical and organizational measures that are also recognized as benchmarks in other jurisdictions. In addition, we comply with the requirements of the international information security standard ISO/IEC 27001 and requirements of personal data protection laws in different countries, including PIPL[1], CCPA[2], LGPD[3], PDPD[4] and Federal Law No. 152-FZ[5].

Five key principles for working with user data:

1. Legality and transparency of data processing for data subjects
2. Legitimacy of the purposes of data processing
3. Refusal to collect redundant data
4. Compliance with data storage deadlines
5. Reliable data protection

We strive to reduce the number of incidents to zero. In the reporting period, we did not commit a single violation of laws on personal data or have any data leaks. This was possible due to regular employee training, the information security technologies that have been introduced, and standardization of data processing. During the reporting period, we updated our data processing requirements and also adapted them to be in line with the laws of different countries.

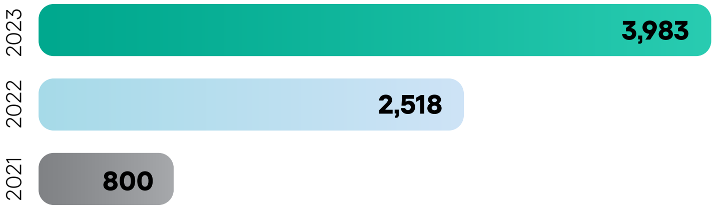
We compile the most current information, including the number of requests from our users that have been satisfied, in a transparency report. The document is publicly available, updated and published every six months.

[1] Personal Information Protection Law of the People's Republic of China.
[2] California Consumer Privacy Act.
[3] Lei Geral de Proteção de Dados (General Personal Data Protection Law).
[4] Personal Data Protection Decree of Vietnam.
[5] Federal Law of the Russian Federation No. 152-FZ dated July 27, 2006 "On Personal Data".

Ensuring responsible management of data

Kaspersky has an awareness course for employees who are directly involved in the processing of customer data. In 2023, 3,983 people completed this course, including all of the our European employees and workers worldwide who are involved in processing and protecting customer data, an increase of 58 percent from the previous year.

Number of employees who completed the awareness course



Risk assessment

We take a risk-based approach to the protection of our users' data. Risk assessments are conducted at all stages: when introducing new systems, developing new solutions and investigating incidents. In each case, we analyze in advance what risks may arise when processing customer data and minimize them.

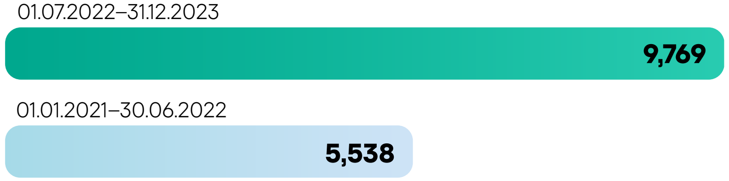
The requirements of the GDPR and regional legislation take into account the risks that users may be exposed to. The ISO/IEC 27001 standard helps us mitigate reputational and financial risks for the Company.

Prompt response to privacy enquiries from our users

TC-SI-220-a.1

Kaspersky receives thousands of requests for data processing from users each month, 90% of which are requests to remove their data from our databases.

Number of requests received from users over the reporting periods[1]



Users are also asked to upload their data, what information about them is stored and where it is stored. We successfully processed 9,769 requests during the reporting period (from July 1, 2022 to the end of 2023) and 5,538 requests in the period from January 1, 2021 to June 30, 2022. We are seeing the number of such requests increase both in Europe and around the world. This is happening for two reasons: growing user awareness about their rights and the adoption of new laws on personal data.

Our goal is to provide all the necessary information about data to users so that they can trust Kaspersky and its products. As part of our streamlined inquiry process, we create transparency reports that document the number and types of requests we receive from customers. We update and publish such reports every six months.

Like most companies, we work with user data and targeted advertising[2]. Per the GDPR, data obtained via cookies[3] is considered personal, which means that the relevant rules must be followed when collecting it. Brazil, the UK and Europe have uniform, strict policies to obtain consent for the collection of information on websites. In other countries, we collect minimal data to provide the relevant information to our potential customers.

To interact with consumers, customers and suppliers, Kaspersky has a feedback form on its official website:

www.kaspersky.ru/about/contact — for Russian users

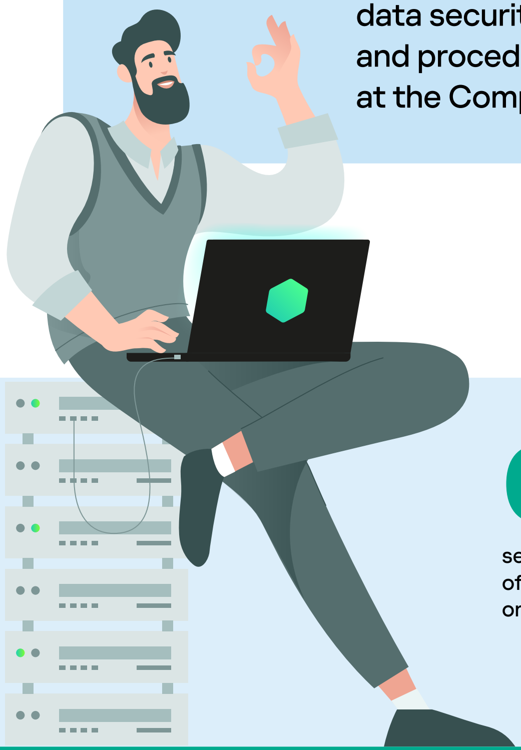
www.kaspersky.com/about/contact — for international users

[1] Per transparency reports.
[2] Targeted advertising is a key marketing tool that is used to collect users' personal data through various websites, applications and social networks in order to promote goods and services.
[3] Cookies are small files stored on computers and gadgets that websites use to remember information about user visits.

Preventing risks of user data processing

GRI-418-1 TC-SI-220-a.1 TC-SI-230-a.1 TC-SI-220-a.2 TC-SI-220-a.3

The Privacy Team is responsible for compliance with data security principles and procedures at the Company.



The Privacy Team, which includes employees from the IT, Research and development, information security and intellectual property departments, was formed in 2016, when GDPR requirements were being introduced. The team brought all the Company's processes into compliance with European regulations. It now performs data processing functions in areas such as consulting, organizational issues and control.

Since 2019, Kaspersky has annually certified its data processing systems for compliance with the requirements of the international standard ISO/IEC 27001, thereby verifying their high level of protection. The scope of the information systems audit was significantly expanded during the reporting period. We hired new staff and formed a new unit, which helped to complete 388 internal audits in 2023.

The scope of certification extends to Kaspersky's data processing function "Delivery of malicious and suspicious files and static activity data using the Kaspersky Security Network (KSN) infrastructure, the safe storage and access to the Kaspersky Lab Distributed File System (KLDFS) and the KSNBuffer database."

The certification is valid for data processing services located at data centers in Beijing, Frankfurt, Glattburg, Moscow, Toronto and Zurich.

Launch of a new tracking system

During the reporting period, we completed an ambitious project: the launch of a new system for tracking processes and data processing services, which was created by the Kaspersky development team. It tracks which services process customer data, which business processes they are used in, the controller (operator) and processor of the data, what data is stored in the system, for how long, on what basis, to what extent and in what countries, etc. The new system is ready for operation and 80 percent of the data has already been transferred to it.

0
serious violations of personal data legislation or major leaks

0
losses as a result of litigation due to violation of confidentiality during the reporting period

388
internal audits
for certification of compliance with ISO/IEC 27001 in 2023

Our plans for 2024

- Presentation of updated requirements for data processing and protection for all services that process customer data.
- Review of the updated requirements with responsible teams.
- Audits on the effectiveness of user data processing and protection services.