

Safeguarding users' trust

Kaspersky creates an environment in which users, customers, and partners can be confident in the security and reliability of the products and services provided by the Company.

Customer service

The trust of users and customers is the foundation of Kaspersky's long-term growth. The Company organizes all processes to ensure that interaction with the Company is convenient and clear at every stage: from choosing and using a product to communicating with customer support and getting a response. Our approach is based on respect for our clients, attention to their needs, and our desire to respond quickly and correctly in every situation.

Interaction with consumers

To effectively interact with consumers, clients, and suppliers, Kaspersky has a feedback form on the Company's official websites:

www.kaspersky.ru/about/contact – for Russian-speaking users

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

For different types of inquiries—including product purchase questions, technical support, and partnership requests—dedicated channels and specialized teams are in place. This approach enables prompt handling of each case and ensures the most appropriate solution is provided.

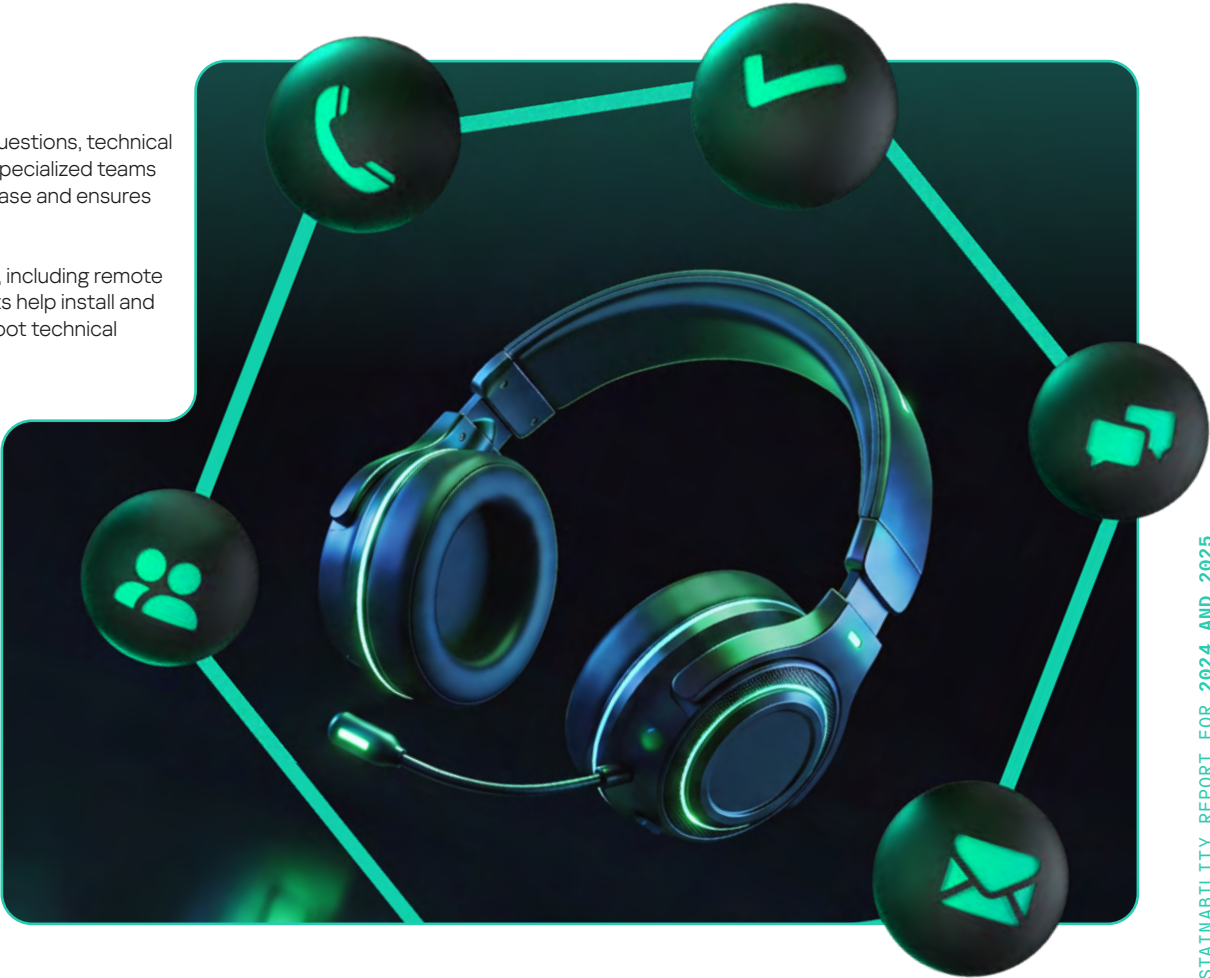
The Company's clients have access to 24/7 technical support, including remote assistance for users of our consumer products. Our specialists help install and configure solutions, scan systems for malware, and troubleshoot technical issues, ensuring stable and uninterrupted protection.

Handling complaints

GRI 2-25

If a client has questions, complaints, or suggestions, they can contact us using the form on the website, by email, phone, or other available channels. All communications are recorded and tracked, allowing us not only to respond promptly to each situation but also to identify recurring issues so they can be addressed systematically rather than on a case-by-case basis.

The team that handles complaints first seeks to understand the nature of the complaint and the reasons for the customer's concern, and then offers a clear, transparent and well-founded solution. The goal of this approach is not simply to formally close support tickets, but to restore trust and rebuild the client's confidence in the quality of the Company's services and products.



Data protection

GRI 3-3

We respect our clients' privacy rights and protect their data. Our goal is to prevent data leaks at Kaspersky and to help our customers combat them with our solutions.

>1.835

user data processing requests in 2024–2025

GRI 418-1

0

user data leaks during the reporting period

Key objectives

- Ensure the protection of customer data worldwide using information security best practices and taking into account local regulations
- Respond promptly to customers' requests regarding the processing and protection of their data
- Prevent unauthorized access to and leaks of user data

Data protection priorities in 2024–2025:

- Implement updated information security requirements in the Company's services
- Protect against supply chain threats
- Use AI to protect the Company's services
- Expand protection of critical services against DDoS attacks
- Launch a new bug bounty program¹

Our approach to data protection

SASB TC-SI-230-a.2

Kaspersky is committed to protecting the data of its customers worldwide. In today's world, data is a valuable asset for companies, so data security and integrity are of paramount importance. We protect our customers' personal information² from unauthorized access and modification using best-in-class technologies and a comprehensive set of technical and organizational security measures.

The Company continuously monitors changes in legislation regarding the processing and protection of personal data in various jurisdictions and implements special projects aimed at bringing processes and systems into compliance with current requirements.

Most countries around the world use a risk-based approach when developing measures to protect personal data. However, in several states, a list of mandatory personal data protection measures is clearly established. The specified requirements are formalized and applied to the Company's services. In particular, these include the following technical measures:

- restriction of access to data;
- timely installation of updates and security patches;
- antivirus protection;
- registration and monitoring of events;
- network protection;
- data encryption;

- fault tolerance and backup copies.

We also implement organizational measures to protect data, including:

- limiting the amount of personal data collected;
- data anonymization;
- development of secure products and prompt elimination of identified vulnerabilities;
- use of digital certificates;
- separate storage of data on multiple servers.

How we protect data globally and prevent data leaks

SASB TC-SI-220a.1

We adhere to the key data processing principles set out in the European Data Protection Regulation (2016). This legislative act sets forth fundamental technical and organizational measures that are also recognized as standards in other jurisdictions. We also comply with international information security standard ISO/IEC 27001 as well as the privacy laws of various countries, including the PIPL, CCPA, LGPD, PDPD, Federal Law No. 152-FZ, and others.

Personal data is stored no longer than is necessary to achieve the purposes of processing that data, or for the periods established by applicable law. Up-to-date information on the countries where data is processing, data access procedures, and data storage periods is available in the current version of the Company's [privacy policy](#).

¹ A program for reporting software bugs and vulnerabilities, typically announced by developers of applications and online platforms to identify security issues in their products. Typically, the program rewards enthusiasts for reporting exploitable bugs. The incentive may sometimes include access to a paid online service or recognition in the professional community.

² Personal data is any information related to an individual, including their full name, telephone numbers, physical address, IP address, email address, etc.

Five key principles of working with customer data:

 Ensure that data subjects' data is processed lawfully and transparently

 Ensure that data is processed for legitimate purposes

 Do not collect excessive data

 Comply with data retention time limits

 Ensure reliable data protection

We strive to prevent all information security incidents. During the reporting period, no violations of personal data legislation and no data leaks were recorded. These results were achieved through our systematic efforts to train employees, implement state-of-the-art information security technologies, and standardize data processing.

During the reporting period, we updated our data processing requirements and adapted them to the laws of various jurisdictions.

Up-to-date information, including the number of granted user requests, is provided in our [Transparency Report](#). This document is publicly available, regularly updated and published every six months.

We teach rules for working with data

Kaspersky has an information security awareness program for employees who work directly with customer data. As of 2025, the program covers all current employees of the Company.

The training combines online and offline activities and aims to develop consistently safe behavior. As part of the program, employees learn the rules for working with personal data and trade secrets, the basics of safely using artificial intelligence services, and also undergo practical training on how to recognize and respond to phishing and fraudulent attacks.

Starting in 2025, the program also extends to new outsourcers and contractors that have access to Kaspersky information systems, ensuring a unified approach to information security across all participants in work processes.

We assess risks

We take a risk-based approach to protecting our users' data. Risk assessment is carried out at all key stages of work—when new systems are deployed, when solutions are developed, and during incident investigations. In each case, we first analyze the potential risks associated with processing customer data and then take measures to minimize those risks.

The requirements of the GDPR and regional legislation are based on an assessment of the risks that users may be exposed to. By using international standard ISO/IEC 27001, we further reduce reputational and financial risks for the Company.

We prevent customer data leaks

GRI 418-1

SASB TC-SI-220-a.1

SASB TC-SI-230-a.1

SASB TC-SI-220-a.3

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

As part of complying with GDPR requirements, the Company established and operates a Privacy Team, which includes employees from the IT, R&D, Information Security, and Intellectual Property departments. In 2016, the Privacy Team brought all data processing into compliance with European regulations. Today, it provides data processing functions in areas such as consulting, organizational issues, and control.

Kaspersky regularly demonstrates the reliability and integrity of its engineering practices through independent audits. In 2025, Kaspersky [reinforced](#) its security credentials by re-certifying its information security management system (ISMS) against ISO/IEC 27001:2022, an international standard which outlines the best practices for establishing, implementing and continuously improving these systems. During the reporting period, the scope of information systems audits expanded significantly: [ISO/IEC 27001](#) and SOC 2 Type 2 audits were conducted on a regular basis, and in 2025, an additional external audit was conducted for compliance with the requirements of the Cybersecurity Regulatory Framework (CRF) of the Kingdom of Saudi Arabia.

The certification covers Kaspersky's data processing for "Delivery of malicious and suspicious files and static activity data using Kaspersky Security Network (KSN) infrastructure, and their secure storage and access in the Kaspersky Distributed File System (KLDFS) and to the KSNBuffer database."

The certification applies to data processing services hosted in data centers located in Zurich, Frankfurt am Main, Glattburg, Toronto, Moscow, and Beijing.

0

serious violations of personal data laws and 0 significant leaks

0

losses resulting from litigation due to privacy breaches during the reporting period

46

internal information security audits were conducted in 2024–2025

We are developing a record-keeping system for data processing procedures

We continue to develop our record-keeping system for data processing procedures and services, which the Kaspersky development team created in 2023. The system makes it possible to track which services process customer data, which business processes use it, who acts as the data controller (operator) and data processor, what data is stored, on what legal grounds, in what volume, and for how long, and which countries the data is processed in.

During the reporting period, we updated personal data processing requirements, communicated them to services, and monitored compliance with these requirements.

Our plans for 2026

- Monitor changes in personal data legislation in various countries and align our processes with current requirements.
- Establish updated data processing and data protection requirements for all services that process customer data, and monitor compliance with these requirements.
- Consult with teams regarding updated requirements and data handling practices.
- Audit the effectiveness of services in relation to the processing and protection of user data.

Protection of intellectual property

We constantly develop and implement advanced cybersecurity solutions, and regularly patent our inventions and innovative technologies.

How we protect and defend intellectual property

One of the most important components of the growth and stability of our business is our intellectual property rights. We protect our innovations and also respect other companies' rights to their technologies and solutions.

Task

Protect and defend rights to products, solutions, and technologies

Solutions

We obtain patents in various jurisdictions

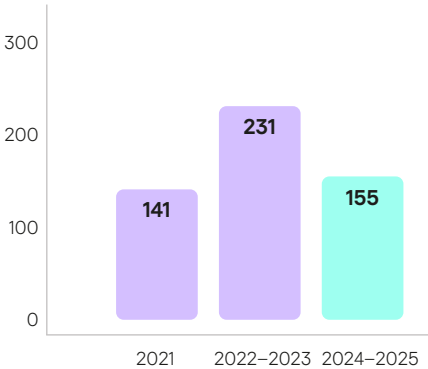
SASB TC-SI-520-a.1

Kaspersky consistently obtains state-protected exclusive rights to the results of its intellectual activity. If a violation occurs, we are prepared to defend our rights in court. This helps uphold the principles of fairness and legality in the business environment.

Between 2024 and 2025, the Company received 155 patents for its technologies in various jurisdictions. In recent years, the focus of patenting has shifted towards B2B products and KasperskyOS, and covers, among other things, machine learning technologies and the use of large language models (LLM) to solve information security problems. Additionally, during the reporting period, we increased the number of patent applications related to the design of our products, including user interfaces.

The protection and defense of intellectual property (IP) has been an integral part of Kaspersky's activities since 2005. In this time, we have established and optimized processes for obtaining legal protection for any results of intellectual activity. In a significant achievement, the Company has not lost any patent lawsuits brought against us by patent trolls¹.

Number of patents received for Kaspersky products



Kaspersky received

155

patents for its technologies in 2024-2025

¹ An individual or entity whose business consists solely of receiving royalties for the use of its patents, without attempting to put the patented inventions into practice.

Along with protecting our own innovations, we devote significant attention to preventing risks associated with the unauthorized use of third-party IP within the Company. This also applies to the use of third-party software code. Accordingly, we implement corresponding policies, thoroughly check licenses, and monitor compliance with all applicable requirements and regulations.

If necessary, we are always prepared to defend our rights in court. This is one of our key strategic positions. We protect our IP using all available legal mechanisms, without resorting to unreasonable settlement schemes. Our goal is a fair and legal dispute resolution that accounts for the interests of all parties.

For example, in April 2024, we concluded a two-year patent dispute in the United States with our direct competitor, the antivirus company Webroot. The dispute was settled on terms that were acceptable to both parties, which allowed us to avoid potential negative scenarios had the dispute continued.

We cultivate an intellectual property culture

Our accumulated experience and expertise allow us not only to effectively protect and defend our own innovations but also to cultivate an intellectual property culture within the Company.

An important part of this work is keeping employees trained and informed. Every new Kaspersky employee undergoes a special introductory training course that gives them a basic understanding of the principles of intellectual property and rules for working with it.

In January 2025, we also launched a specialized course on patents for employees in our technical departments. It helps employees understand the basics of patenting and how intellectual property protects innovations and promotes business growth. During the course, employees

involved in new product development not only gain basic knowledge of patent law but also learn information about the Company's internal procedures related to intellectual property protection.

During the reporting period, our internal platform published significantly more content dedicated not only to patenting, but also to other objects of intellectual property.

In addition, we place strong emphasis on supporting employees who are pursuing higher education and wish to use Kaspersky's intellectual property in their academic research. Each of these employees receives the necessary expert support to carry out research initiatives while protecting critical information.

Our plans for 2026

- Expansion of the geographical scope of patent protection to additional jurisdictions, along with an increase in the total number of patent applications filed.
- Monitor changes in the legal landscape to promptly review local IP regulations and develop new documents to address current issues.
- Development of employee training and awareness programs, including the creation of resources and guidelines on intellectual property for employees who are students at higher education institutions. This will help ensure compliance with the Company's rules and policies.
- Increase the level of automation of internal processes related to intellectual property.

We maintain a high level of internal efficiency

As the range of tasks related to intellectual property expands each year, it becomes especially important to increase efficiency of processes and automate them. Several relevant initiatives were implemented in 2024–2025.

1

We continue to develop an automated system for analyzing software and other objects with open-source and free licenses. During the reporting period, we designed and implemented a separate module that efficiently identifies licensing terms and generates copyright information for open-source software used in the Company's products. This has significantly accelerated the legal review of our products and services and ensured compliance with global best practices for working with open-source software.

2

We revised the process for publishing open-source projects that give the developer community access to our technologies. We created well-structured and clear guidelines for development teams, which reduced the likelihood of errors when publishing code and also reduced excessive communication with the department responsible for intellectual property issues.

3

During the reporting period, we deployed an LLM assistant that helps speed up the analysis of patents from foreign jurisdictions and optimizes work in this area.



Global Transparency Initiative

Our goal is to provide the necessary tools and conditions for our corporate clients, partners, and regulators to verify the integrity and reliability of our products.



What is the Global Transparency Initiative?

The Global Transparency Initiative (GTI) is a system of measures aimed at increasing the transparency and reliability of Kaspersky's products, development processes, and business processes. GTI provides customers, partners, and regulators with access to information about product architecture, data management, and security procedures, including the ability to review source code at dedicated transparency centers. External experts provide feedback that helps us improve processes and ensure that our solutions maintain a high level of maturity.

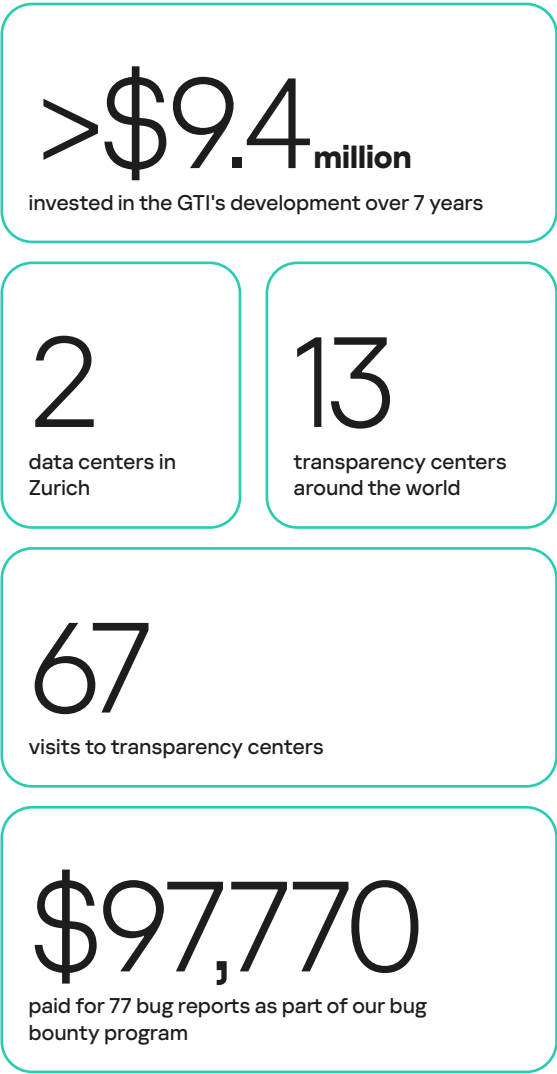
How the GTI came to be and how it has evolved

The Global Transparency Initiative was launched in 2018 in response to requests from regulators and customers seeking greater insight into how our products work, including how data is processed and stored. Today, GTI is a comprehensive system that combines independent audits, source code analysis, educational initiatives, and the development of data processing infrastructure.

- As part of the GTI, the Company:
- introduced independent analysis of source code, updates, and threat detection rules;
 - introduced independent assessment of secure development and risk management in the supply chain;
 - introduced independent assessment of secure development and risk management in the supply chain;
 - improved the bug bounty program;
 - moved part of the infrastructure for storing and processing suspicious files to data centers in Switzerland;
 - began publishing reports on requests from law enforcement agencies and government agencies;
 - developed programs to enhance competencies in IT infrastructure security, such as the Cyber Capacity Building Program.

In 2025, Kaspersky celebrated the seventh anniversary of the Global Transparency Initiative. Over its lifetime, the GTI has evolved into a full-fledged transparency system.

Seven years of results from the GTI



How does the GTI work?

Basic elements of the GTI

- 1. Source code access for clients and regulators**

An important element of the system is independent verification of the source code of Kaspersky products. In addition, several stakeholders can receive information about the source code of the Company's main products and our data processing principles.
- 2. Cooperation with the expert community**

We invite independent experts from around the world to test our systems and products, which creates even more confidence in their reliability.
- 3. Educational activities**

The Company's educational initiatives under the GTI aim to raise awareness among users and partners about the importance of security in the digital world.

How we ensure that our products and business processes are transparent

Task

Strengthen public trust in the Company's products and activities

To build trust with our clients, partners, and regulators, we continually grow the GTI's infrastructure, disclose information about our processes, undergo audits, obtain certifications, and improve security standards.

Key solutions

We are expanding our data processing infrastructure

In 2018, Kaspersky began moving the processing and storage of suspicious and malicious files to two data centers in Switzerland that operate under strict data protection regulations. As a result, data voluntarily shared by users from Europe, North and Latin America, the Middle East, as well as several countries in the Asia-Pacific region is now processed in Zurich within the Kaspersky Security Network cloud system.

We are expanding the network of transparency centers

Transparency centers allow our corporate clients, partners, and government regulators responsible for cybersecurity to examine the source code of the Company's products and learn more about its internal processes. The first center was opened in Zurich in 2018. In just seven years, we established 13 transparency centers in Brazil, Italy, Japan, Malaysia, the Netherlands, Rwanda, Saudi Arabia, Singapore, Spain, Switzerland, [Turkey](#), [Colombia](#) and [South Korea](#). Three of them were opened in 2024–2025.



13
transparency
centers
around the world

2
independent SOC
2 and ISO 27001
compliance audits

We launched a GTI
course for partners.

The GTI's results for 2024–2025

3
new transparency
centers were opened
in Istanbul, Bogota
and Seoul

7
The Company's
products were
reviewed 7 times at
transparency centers

>\$15.000
paid for 18 bug reports as part of our bug bounty
program



We are assessed independently

Kaspersky regularly obtains independent assessments and proves that its internal processes are secure. Since 2019, the Company's data management systems have been certified as compliant with the [ISO/IEC 27001:2022](#) standard and passed [SOC 2](#) audits. In 2025, Kaspersky's information security management system was [recertified](#) as compliant with the ISO/IEC 27001:2022 standard, which confirms that it is secure.

In [2024](#) and [2025](#), the Company again successfully passed a SOC 2 Type 2 audit. The audit demonstrated that Kaspersky's internal controls, which ensure regular automatic updates of anti-virus databases, are working effectively, and that our process for developing and releasing anti-virus databases is protected from unauthorized interference.

In 2024 and 2025, we successfully passed two SOC 2 Type 2 audits.



We collect data on vulnerabilities through a bug bounty program.

Since March 2018, Kaspersky has received 77 reports of minor vulnerabilities through our bug bounty program, fixed them and, as of today, paid out bounties totaling \$97,770 to independent researchers. The maximum reward for critical vulnerabilities is \$100,000.

Since 2022, the Company has been running its public bug bounty program on the [Yogosha](#) platform. We also support [Disclose.io](#), which provides a safe space for vulnerability researchers concerned about the potential legal repercussions of their disclosures.

77

bug reports received in 7 years

\$97,770

paid for bug reports



We teach how to assess the cybersecurity level

Our educational [Cyber Capacity Building](#) Program helps employees of private and public companies, as well as universities, develop skills in assessing the security level of IT infrastructure. As part of the program, our specialists provide recommendations on code auditing, creating procedures for handling vulnerabilities, and code fuzzing techniques¹.

During the reporting period, representatives of several organizations, including the National Cyber Security Agency of Thailand and Boğaziçi University (Istanbul), completed the training.

In 2025, our Cyber Capacity Building Program was selected by the World Internet Conference (WIC) as an one of the Outstanding Cases of Jointly Building a Community with a Shared Future in Cyberspace.



We publish transparency reports

Our mission is to protect users from cyberthreats, which is why we support our partners, international organizations, and law enforcement agencies in the fight against cybercrime. We regularly process requests and, since 2020 we [have published reports](#) featuring information about the number of such requests by country, as well as how many we granted and rejected. Accordingly, the Company has a procedure for processing these requests, including, in particular, clear criteria for verifying their legality.

Every six months, Kaspersky discloses the number of law enforcement and government requests for user data, expertise, and threat intelligence data. However, we do not provide any third parties² with access to the Company's infrastructure, including the data processing infrastructure. We also regularly report on requests from our own users regarding their personal data, how we process it, where it is stored, and so on.

¹ A software testing method where a program is given deliberately incorrect data, the response is analyzed, and any resulting bugs are detected.
² Learn more about how we handle requests in our [transparency reports](#).

Our contribution to promoting the ethical and safe use of AI in cybersecurity

Artificial intelligence allows new cyberthreats to be detected and neutralized more effectively, but its use carries risks for privacy, data security, and user rights. In 2024–2025, Kaspersky stepped up its efforts to develop and promote ethical standards for the use of AI in the digital world.

What we did

- [We presented](#) the Guidelines for Secure Development and Deployment of AI Systems at the UN Internet Governance Forum (IGF) 2024 in Riyadh. The purpose of the document is to help organizations avoid cyber risks associated with the use of AI technologies.
- [We formulated](#) clear relevant guidelines for stakeholders: from threat modeling and risk assessment to protection against AI attacks and compliance with international regulations, such as the GDPR.
- [We signed](#) the European Commission's Artificial Intelligence Pact (AI Pact), confirming that we are prepared to build an AI governance strategy that is aligned with the logic of the future EU AI Act¹.
- [We committed to](#) adopting an internal AI governance strategy and raising awareness among employees and others about interactions with AI.
- [We joined](#) the Global Alliance on AI for Industry and Manufacturing, established in 2023 by the United Nations Industrial Development Organization (UNIDO), and the AI Alliance Russia (a-ai.ru), which unites leading Russian technology companies for the purpose of responsible AI development.
- We reaffirmed our [principles](#) for the responsible use of AI in cybersecurity: transparency, safety, human control, the right to digital privacy, a commitment to cybersecurity objectives, and openness to dialogue.

Our achievements

- We strengthened Kaspersky's role as a leader in setting global standards for ethical AI in cybersecurity.
- We became an active participant in the pan-European discussion on AI regulation and prepared the Company to comply with the EU AI Act.
- We communicated to partners, clients, regulators, and the professional community how we ensure the reliability and security of AI systems and invited them to develop shared ethical principles for digital development.

GTI plans for 2026–2027

- Possibly expand the network of transparency centers (APAC)
- Diversify data centers, expand infrastructure for processing malicious and suspicious files
- Continue to invite stakeholders to transparency centers
- Recertify compliance with key standards
- Continue to publish reports on data requests

¹ The EU AI Act comes into force in mid-2026. This is a European Commission initiative aimed at creating a common regulatory framework for the use of AI.