kaspersky

Security, reliability, trustworthiness, transparency, and quality:

What you can rely on with Kaspersky, and how you can check up on it!

Since the warning of the German Federal Office for Information Security (BSI), questions have arisen as to the reliability, trustworthiness and security of Kaspersky and its antivirus software (AV). With this paper, we would like to answer these questions transparently and provide you with information on:

- how Kaspersky plans, organizes, and implements the principles of security, availability, confidentiality, and privacy in software development and distribution;
- how the company undergoes external certification in accordance with internationally recognized standards;
- how Kaspersky defines transparency and how this concept applies in the company's relations with customers, partners, and other stakeholders.

*As an **international cybersecurity company,** Kaspersky makes valuable contributions to **cybersecurity and resilience** in Germany, the DACH region, Europe and worldwide.*

*Kaspersky is a **privately held company.** The **group holding is based in London (UK).***

***Legally independent national companies** are active in the various countries; e.g., Kaspersky Labs GmbH in Germany.*

*Kaspersky Labs GmbH pays its **taxes, social security contributions and wages** in Germany and **invests** in research and development.*

*Kaspersky employs around **700 people** in **Europe** alone. Its **Global Research and Analysis Team (GReAT)** is managed from Bucharest. Most GReAT researchers are based in the EU.*

Despite the current geopolitical situation and the BSI warning, Kaspersky provides all contractually agreed services of the best quality, completely and without any restrictions. In particular, all Kaspersky software is working perfectly, has no technical shortcomings *(this is also confirmed by the BSI and the Münster Higher Administrative Court (OVG); see p. 2)* and provides the highest possible levels of protection. This is also certified by numerous independent external tests.

Certified and audited security and safety

On its homepage, the BSI writes: *"With the help of a certificate, an organization can prove that a product or service meets defined security requirements. An independent audit by the BSI creates trust and transparently demonstrates confidentiality, authenticity and availability."* Kaspersky shares this view, and regularly undergoes comprehensive certifications in accordance with internationally recognized standards. Kaspersky's enterprise solutions were certified according to Common Criteria in Spain and Italy. In addition, Kaspersky passed ISO 27001 certification. What is more, one of the Big Four global accounting firms audited Kaspersky's software development and distribution processes in 2019 and again in 2022 (finalized April 28), in accordance with SOC 2 Type 1 under the guidelines of the standard developed by the American Institute of Certified Public Accountants (AICPA Professional Standard).

How the software is made up

Kaspersky provides customers, partners, and regulators with a Software Bill of Materials *(SBOM).* This is a list of all software components. It consists of supporting documents that describe the parts that make up a piece of software. SBOM provision is an ever more common best practice within the industry; it increases the transparency of software and improves the visibility of software composition and architecture to help build a reliable and trustworthy digital infrastructure.

kaspersky

Analysis of source code in real time – at any time

If you require even more security and transparency, you can analyze and check Kaspersky's source code in a Transparency Center or via secure remote environments. Numerous European authorities, scientific institutions as well as customers and partners have already made use of this option. The reviews require expert IT knowledge from your company or from service providers. Since not just the current software version, but all previous versions can be checked and compared with the delivered version, this check offers the highest level of security available. This practice is the only one of its kind in the AV market worldwide.

The warning issued by the BSI is unique in Europe

To our knowledge (as of May 4, 2022), among all 27 cybersecurity authorities of the EU Member States, only nine have issued statements on the use of Russian software. There is no geopolitical warning comparable to that of the BSI in any other European state. (Some statements are listed in the box on the right).

FRANCE - National Agency for the Security of Information Systems (ANSSI)
"In the current context, the use of certain digital tools, in particular those of the Kaspersky company, may be questioned due to their association with Russia. At this stage, there is no objective reason to change the assessment of the quality of the products and services offered."
Source: https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

SWITZERLAND - National Cyber Security Centre (NCSC)
When asked, the NCSC stated that it is not aware of any misuse on the part of Kaspersky. *"If the NCSC had any evidence in this regard, it would warn and inform the public accordingly"*, writes Pascal Lamia, the centre's operational director.
Source: https://www.inside-it.ch/deutsches-bundesamt-fuer-cybersicherheit-raet,-kaspersky-software-zu-verbannen-20220315

BELGIUM - Centre for Cybersecurity Belgium (CCB)
"The Centre for Cybersecurity Belgium (CCB) also sees no threat at this time."
Source:
https://www.computable.nl/artikel/nieuws/security/7329186/250449/duitse-overheid-waarschuwt-voor-kaspersky.html

AUSTRIA - Austrian CERT (cert.at)
"CERT.at currently has no information that Kaspersky products contain malicious functions."
Source: CERT.at message to Austrian companies

Kaspersky ensures robust, secure and reliable business processes

The Kaspersky team continuously and proactively assesses all potential risks arising from the geopolitical situation and is ready to act swiftly if necessary. In doing so, we also assess the potential impact of restrictions on interstate data exchange on the company's products and services. All tests and investigations to date have shown that Kaspersky's global server infrastructure allows its portfolio to operate without interruption, and that the Kaspersky Security Network (KSN) for processing cybersecurity data is not affected. The data infrastructure is distributed all over the world, including in Switzerland, Germany, China, and Canada. Availability, continuity and processing speed of the servers meet the highest standards. Cyber threat-related data that Kaspersky users in Europe voluntarily share with KSN for automatic malware analysis is only sent to European servers.

BSI recommends individual risk analysis
On its website, the Federal Office points out that each institution should conduct an individual risk analysis. The decision as to whether a company or an authority wants to use Kaspersky or not must therefore be made by each institution itself according to an individual risk analysis. The Higher Administration Court of North Rhine-Westphalia writes in its decision that the BSI makes it clear in the warning that there are no concrete indications ***"that data was tapped without authorisation with the help of Kaspersky's virus protection programmes or that facts are otherwise known that the software has already been misused. It is also clear that the warning is not based on concrete technical defects in the virus protection programmes distributed by the applicant."*** In addition, the Higher Administration Court makes clear that ***"the Federal Office warns against the use of the virus protection software of the manufacturer Kaspersky due to the current geopolitical situation and the associated risks of a Russian cyber attack".***

You can continue to rely on Kaspersky as a dependable contractual partner and powerful IT security provider now and in the future!