

# Statement of Kaspersky on the BSI warning according to § 7 BSI G

We have sent the following response to the BSI after they have published a warning:

We consider the BSI recommendation to be unjust and not based on objective technical analysis of the risks of using Kaspersky software and solution. **A warning sent on March 15, 2022 without sufficient time for Kaspersky to comment in detail cannot be nor procedurally technically justified when dealing with the one of the world's largest and most reputable cybersecurity companies, and a long-time partner for BSI.**

In particular:

- The BSI states in the warning; "In the case of the anti-virus protection software distributed by Kaspersky, the BSI comes to the conclusion that a high risk can currently arise from the further use of this product simply because the system rights granted for the anti-virus protection on the target systems to be protected are subject to manipulation and misuse enabled by Kaspersky and/or third parties."

**This statement not only applies to Kaspersky software, but also to all anti-virus software available on the market. Kaspersky has been continuously taking steps to ensure transparency and integrity of our products, including inviting BSI and other interested organizations to review our source code, updates, and software architecture at the Transparency Center in Zurich, and since March 2022 – in remote format.**

- The BSI also writes: Since there are sufficient indications that the anti-virus protection from Kaspersky poses a threat to information technology security, the BSI can, in fulfillment of its statutory duties, warn against the use of the product and make recommendations (§ 7 Para. 2 BSI G).

**The BSI does not disclose what indications may represent threats to the security of information technology. Kaspersky's risk of state interference from the Russian government is significantly lower than that of any other cybersecurity company in the world. Kaspersky has implemented technical, infrastructural, organizational and corporate measures to enhance its transparency and security for more than ten years and these measures are continuously audited and certified by the respected organizations.**

- In addition, the BSI writes: Due to the special security situation, there is a risk of delay. The BSI therefore considers an immediate reaction to be appropriate.

**If there is imminent danger, then such danger applies not exclusively to Kaspersky software, but to all security-related software and hardware that is used in Germany. More so, the immediate removal of security software will only expose customers to the real and present danger of cyberattacks, which represent a far greater risk than any speculative scenarios of a third-party interference. We are continuously taking steps to prevent any interference with Kaspersky products, and these efforts were audited and certified as sufficient by the independent third-party audits and assessments. We invite the BSI to conduct its own assessment of this in our transparency centers or in a remote format.**

- According to Section 7 (1) BSI G, the BSI may warn against security gaps in information technology products and provide information to the public about security-relevant IT properties in products.

**While the BSI warns against a possible, potential danger of Kaspersky, these very same gaps apply to all cybersecurity companies, global IT service providers and software products. We would be pleased to identify criteria with the BSI that do justice to the political situation and the threat in cyberspace and seek immediate remediation steps. In fact, Kaspersky remains one of the key contributors of information on vulnerabilities of critical software and hardware systems, including those of the leading German companies. The decision to cut the ties with Kaspersky will not make German businesses safer – in fact, quite the contrary, since the vulnerabilities in third-party software will remain undetected or unreported.**

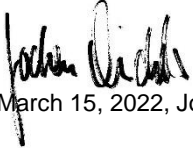
We want to reiterate that we fully understand the political concerns about the conflict in Ukraine. However, notwithstanding the political risks, the only objective way to address those risks lies in technology, its transparency and validation measures – something that we have been advocating for with BSI for years. We sincerely ask you to consider our arguments, conduct comprehensive reviews and make a fact-based decision to strengthen cybersecurity and resilience in Germany. We have attached further documents for your consideration.

As a global cybersecurity company, Kaspersky is since more than 20 years a trustworthy contributor to the cybersecurity ecosystem in Germany and the European Union as a whole. Kaspersky is a private international company and our local businesses are run by local entities, which gives us the opportunity to effectively and independently control international and local operations. The company operates in more than 200 countries and territories.

Kaspersky is not subject to the Russian System of Operational Investigative Measures (SORM) or other similar legislation and is therefore not obliged to provide information. This has been confirmed by an independent third-party legal assessment of Russian data processing legislation. **The results are freely available online and provide an unbiased and fair legal assessment. More so, we clearly stated that our key Transparency principle is that no third-party access to our data or infrastructure is ever allowed, and requests for undeclared functionality are always declined.**

It is our main goal and driving motivation to protect Germany's citizens, companies, and public authorities in the best possible way. We remain open and committed to dialogue and greater scrutiny of Kaspersky products and operations from BSI and other interested parties.

We work to make the cyber world safer – and taking politicized and unwarranted decisions against a company that for 25 years has been spearheading the global fight against cyber threats of all sorts goes against ours – and BSI's – mission.



March 15, 2022, Jochen Michels, Head of Public Affairs Europe, Kaspersky