kaspersky

# Warning of the BSI
# due to the current geopolitical situation

***With this special impulse paper for Germany, we would like to initiate a more in-depth professional discussion with the community of lawyers specializing in IT law, IT security law, data law, and data protection law. Background: According to research done by Kaspersky, no warnings have been issued in Europe comparative to the BSI warning. Further, there is now a new interpretation of the term "security gap" in Europe comparable to the German one. Therefore, we are particularly interested in experts' dialog in Germany.*** ***We look forward to your thoughts, arguments, ideas, and feedback!***

As an **international cybersecurity company,** Kaspersky makes numerous 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 ca. 700 **employees in Europe.** Its **Global Research and Analysis Team (GReAT)** is controlled from Bucharest. Most GReAT researchers are based in Europe.

The Higher Administrative Court for the state of North Rhine-Westphalia (OVG) states in its decision 4 B 473/22 from April 28, 2022 on the legality of the BSI's warning of March 15, 2022 against Kaspersky's antivirus (AV) software:

*"The Federal Office made the decision to issue the warning without any error of judgment and, in particular, complied with the principle of proportionality. The warning was not issued on the basis of extraneous considerations; in particular, it was neither politically motivated nor does it represent pure symbolic politics."*

The decision was received critically by experts. Prof. Dr. Dennis-Kenji Kipker of the University of Bremen wrote in a first reply:

*"The reasoning for this decision is – with due respect – a legal catastrophe and actually itself an irrelevant consideration." (Source: https://community.beck.de/2022/04/28/bei-virenschutzprogrammen-bestehen-schon-aufgrund-ihrer-funktionsweise-sicherheitsluecken-ovg-nrw-zur-warnung; visited on May , 2022, 7.30 CET)*

Kaspersky regrets the decision of the Higher Administrative Court (OVG) for the State of North Rhine-Westphalia from April 28, 2022, to reject the appeal of Kaspersky Labs GmbH against the urgent decision of the Administrative Court of Cologne (VG) of April 1, 2022, thus classifying the warning of the Federal Office for Information Security (BSI) against the use of Kaspersky's antivirus software as lawful. Kaspersky, its lawyers, and sections of the expert community consider the decision to be legally questionable and technically unsuitable in view of the objective, namely – to increase cybersecurity and resilience.

kaspersky

## CAN § 7 OF THE BSI-LAW (BSIG) BE A BASIS FOR THE WARNING?

Kaspersky and its legal counsel cannot understand the new interpretation of the term *security gap* by the Cologne Administrative Court (VG) and the North Rhine-Westphalia Higher Administrative Court (OVG) in Münster. The company is of the opinion that neither the factual requirements of Section 7 (1) BSIG nor those of Section 7 (2) BSIG are met. Against this background, Kaspersky cannot see any legal basis for the BSI to issue this warning. Kaspersky, its lawyers, and sections of the expert community do not understand why the OVG NRW and the VG refer to AV software inherently as a security vulnerability due to its far-reaching system authorization. According to Kaspersky, the requirements defined by the judiciary for the competence, reliability and trustworthiness of antivirus programs cannot be derived from the law. If reliability were the only decisive factor, there would have to be certification or licensing for providers of AV software. However, in fact they do not exist.

## IS THE SAME THING BEING TREATED DIFFERENTLY?

The OVG does not consider the warning to be unequal treatment compared to other manufacturers of antivirus programs within the meaning of the general principle of equality (Section 3 (1) of the German Constitution). Kaspersky's lawyers and other legal experts do not share this view. There is no legally sound justification in the decision. In addition, Kaspersky and its lawyers are surprised that the OVG does not address many of Kaspersky's arguments in the decision. Among other things, the OVG writes:

*"The same applies to the applicant's blanket objection that a warning must also apply with regard to the use of software from the USA."*

Kaspersky wrote the following in the immediate appeal:

*"A look at the USA also shows how arbitrary the BSI's warning is. Although the U.S. spied on Chancellor Merkel and there was concrete proof of this, software from the U.S. is apparently classified as completely unproblematic. (...)."*
*(Source: Immediate appeal by Kaspersky dated April 6, 2022 against the decision of the Cologne Administrative Court dated April 1, 2022)*

In addition, Kaspersky had referred to the article by Sven Herpig and Manuel Atug of April 7, 2022 in Tagesspiegel Background Cybersecurity in the immediate appeal as well as in further comments*: "We recall both the extensive compromise of the SolarWinds software from last year and the operation of the US National Security Agency, which became known from the Snowden publications, which provided Cisco products with spy implants before delivery: https://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html*"

Kaspersky and its lawyers cannot understand why the OVG apparently did not take this information into account and are of the opinion that the OVG's reasoning is flawed and that the OVG drew illogical conclusions in several points.

On the one hand, there were and are cases where the BSI did not warn despite evidence, such as in the cases with U.S. involvement described above. On the other hand, the OVG approves in the decision that the BSI warning, even though

- **there is no evidence, only assumptions and possibilities;**
- **the BSI confirms that there is no technical vulnerability in the Kaspersky software;**
- **Kaspersky has implemented by far the highest and most comprehensive security mechanisms in the world and is continuously updating them.**

kaspersky

## HOW CAREFULLY WERE THE FACTS CONSIDERED?

Upon review of the OVG's decision, the factual errors, inaccuracies, the unchecked adoption of sources previously cited during litigation, and illogical conclusion are surprising:

- As evidence of possible pressure from the Kremlin, the 2017 arrest and prosecution of a Kaspersky employee is mentioned. There is no mention that the cause of arrest occurred prior to his employment at Kaspersky.
- The OVG considers Kaspersky's support for law enforcement agencies fighting cybercrime in Russia (specifically, with the FSB), which is always within the framework of applicable laws and exclusively through the provision of technical expertise, to be a sign of Kaspersky's unreliability. In addition, the OVG denounces Kaspersky's failure to distance itself from this cooperation to combat cybercrime, including with Russian law enforcement agencies. However, the OVG does not state that Kaspersky operates exclusively based on applicable national and international law, has defined clear transparency criteria, and voluntarily publishes a transparency report on this twice a year.
- The fact that Kaspersky, as a global company, complies with the respective national legislation and applies national law for Russian users in Russia is not a sign of lawful action, but rather, according to the OVG, inappropriate collaboration with the Russian state.
- The OVG claims twice in the decision that the head of Kaspersky's Global Research & Analysis Team (GReAT) is based in Moscow. In fact, this top security expert at the company is Romanian and works out of Bucharest.

## WHAT IS THE LINK BETWEEN THE GEOPOLITICAL SITUATION AND KASPERSKY?

The court extensively discusses the geopolitical situation. It lists the actions of the Russian military and intelligence forces and refers to the threats recently issued by Russia against the EU, NATO and the Federal Republic of Germany in the course of the current armed conflict in Ukraine. Against this background, the court finds that there is a significant risk of a successful IT attack by Russia. The court does not make a specific reference to Kaspersky. The court also does not consider that the Kaspersky AV software offers effective protection against such cyber threats. Nor does it consider the fact that the assessment of the presented cyber situation is likely to be based, among other things, on Kaspersky's high-quality threat intelligence. In fact, Kaspersky's antivirus software continues to protect the infrastructure and systems of its customers reliably and in top quality – more than two months after the BSI claimed there was immediate danger on March 15, 2022.

## HOW VALUABLE ARE PRODUCT CERTIFICATIONS?

The OVG writes the following in its decision on the usefulness and meaningfulness of certifications and international standards:

*"The Federal Office also did not have to make a different assessment because the security and reliability of Kaspersky's technical and organizational procedures and data services had been confirmed in the past by two external, independent testing organizations. A fundamental challenge of certification is precisely that software is dynamic and requires continuous updates to close vulnerabilities or improve its functionality. Certification is static in principle. It says, as the federal agency aptly points out in its cautionary statement, only something about the current state during the audit but cannot be a guarantee for any future state."*

However, the OVG does not seem to have taken a closer look at the purpose and significance of certifications. The BSI writes on its website:

kaspersky

*"The BSI is THE certification body in Germany, working with national and international partners to advance cyber security worldwide. The BSI's range of certification and recognition services for products, services and individuals makes an important contribution to information security in Germany."*

And:

*"With 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 fully agrees with the statement of the BSI, and has as such repeatedly faced numerous audits, most recently in 2022 according to Common Criteria in Spain and Italy, according to ISO 27001 and currently the re-audit of Kaspersky's software development and distribution processes according to the guidelines of the standard developed by the American Institute of Certified Public Accountants (AICPA) (AICPA Professional Standard). This audit is called SOC 2 Type 1.

## WHAT IS MORE CONVINCING THAN SOURCE CODE AUDITS IN REAL TIME?

For those who want even more security and transparency, the company's source code can be analyzed and audited in a Transparency Center or via secure remote environments. Many European authorities, scientific institutions, customers, and partners have already taken advantage of this. The BSI has not. Without question, the reviews are demanding and require expert knowledge. 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.

## WHY IS THE BSI WARNING UNIQUE IN EUROPE?

To our knowledge (as of May 5, 2022), among the 27 cybersecurity authorities in all EU Member States, only nine authorities have issued information on the use of Russian software. There is no geopolitical warning comparable to that of the BSI in any other European state *(see 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, 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 corporations*

## WAS THERE EVER IMMINENT DANGER?

*"There is an imminent danger due to the special security situation. The BSI therefore considers an immediate response to be appropriate."*

That is what the BSI wrote to the Kaspersky European Headquarters on March 14, 2022, at 1.52 p.m. German time, in its emailed letter from the head of the KM department, with the subject *BSI warning according to Section 7 BSIG: Opportunity to comment under reference number: KM14-210 01 03.*

The warning came without delay. Specifically, on March 15, 2022, 10.00 a.m. German time. It is remarkable that, to date, all Kaspersky customers in Germany, the rest of Europe, as well as worldwide are well protected. There have been numerous actual cyberattacks, from Russia as well as other regions of the world, from state-sponsored APT groups (APT – Advanced Persistent Threat) and other actors. Kaspersky software, on the other hand, was not compromised or used for offensive cyber-operations even two months after the BSI warning. During this time, Kaspersky AV has securely identified, quarantined and removed all types of malware on its customers' devices and infrastructure. Further,

during this time, Kaspersky researchers have made valuable contributions to strengthening cybersecurity with their threat intelligence.

## WHAT SECURITY MEASURES SHOULD KASPERSKY IMPLEMENT IN THE CURRENT GEOPOLITICAL SITUATION?

When asked what the difference is between the BSI warning pursuant to § 7 BSIG and the rest of the BSI's information and other warning products, the BSI answers with the following on its website:

*"In contrast to the BSI's other information products, which generally reference information and measures taken by the manufacturer, at the time of publication of a BSI warning pursuant to Section 7 BSIG, the manufacturer has not taken any, sufficient or timely measures of its own to eliminate or contain the hazard posed by the product."*

*(Source: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/warnungen-nach-par-7_node.html; visited on May 4, 2022 13:28 CET)*

Kaspersky has always had a close professional-technical exchange with the BSI and for many years has continuously and proactively provided information about the technical, organizational and structural measures taken, about qualification initiatives, certifications and audits as well as about the principles and policies of security, availability, confidentiality and data protection applied by Kaspersky in software development and software distribution.

Until the warning of March 15, 2022, the BSI never expressed any doubts as to the adequacy and effectiveness of these measures.

Today, this is no longer supposed to apply due to the geopolitical situation. The OVG confirms that the BSI was correct in stating that all these measures would no longer be sufficient in the current situation. However, neither the BSI nor the OVG say which measures would be sufficient in the current situation. Kaspersky would do everything in its power, in close exchange with the BSI, to fulfil such a list of measures as quickly as possible.