International collaboration, transparency, trust, risk management and local responsibility: five pillars of Kaspersky's DNA

Why you can trust Kasperky, even with the geopolitical situation!

kaspersky

kaspersky

Software development and distribution is protected from unauthorized access!

kaspersky

- **Highest security standards** in the software development and distrubition process of Kaspersky!
- Even if the Russian government were to force Kaspersky to integrate malware, **the multiple nested approval processes** with a highly restrictive role and rights model **prevent**, with **probability bordering on certainty** (the highest possible promise in cybersecurity), **that updates with malware get onto the upload servers!**
- The **distribution processes** involve **teams from all regions of the world,** including **the USA and Canada.**

SOC2 is a “look behind the scenes”

- **Who and how?** The auditor makes an assessment of whether the regulations and measures prevailing at Kaspersky are well implemented and meet the required criteria for trust services **(security, availability, processing integrity, confidentiality, and privacy). Kaspersky** meets **all 72 criteria without qualification.**
- **What?** The subject of the audit is **Kaspersky's development and implementation of antivirus programs for Windows and Unix operating systems.** The audit proves that Kaspersky's process meets the criteria for trusted services.
- **Why?** The **SOC 2 type 1 audit** (system and organization controls) provides third parties (customers, partners, stakeholder) with a transparent view of Kaspersky's software development and deployment processes. It is therefore a look **"behind the scenes".**
- Further information: https://www.kaspersky.com/about/compliance-soc2

Common Criteria (CC)-Certification for KES and KSC

- *The **Common Criteria for Information Technology Security Evaulation** (in short **Common Criteria** or **CC**) is an international standard for testing and evaluating the security properties of IT products.*
- Kaspersky Endpoint Security (KES), the flagship among the company's products, has been certified in Spain according to the Common Criteria (CC). The certification is recognized throughout Europe: https://commoncriteriaportal.org/files/epfiles/2018-37-INF-2718.pdf
- The Kaspersky Security Center (KSC), the control console for our enterprise products, has also been certified according to Common Criteria (CC) in Italy. The certification is recognized throughout Europe: https://ocsi.isticom.it/documenti/certificazioni/kaspersky/cr_ksc13_v1.0_en.pdf

Common Criteria for Information Technology Security Evaluation

- The Common Criteria distinguish between the **functionality (functional scope)** of the system under consideration and **the trustworthiness (quality).**
- The trustworthiness is considered according to the aspects of **the effectiveness of the methods used** and **the correctness of the implementation.**
- In December 1999 the Common Criteria were declared as the International Standard ISO/IEC 15408. The German part of this work is supervised by DIN NIA-01-27 IT Security Procedures, among others.

ISO 27001 certification & re-certification

- The certification covers Kaspersky Data Services (KSN), including:
  - KSN system for secure storage and access to files (KLDFS) and
  - KSN systems for processing statistics (called KSNBuffer database).
- The certification applies to the company's **data services at its data centers** in **Zurich, Frankfurt, Toronto, Moscow, and Beijing.**
- Conformity with ISO/IEC 27001:2013 – an internationally recognized best practice industry and security standard – is at the core of Kaspersky's approach to implementing and managing information security.
- Link to the re.certification of 2022: We are happy to provide the final report to our customers and partners upon request.
- More information: https://www.kaspersky.com/about/iso-27001

kaspersky

Publications from cybersecurity authorities in Europe

The BSI is alone with its warning in Europe!

Other recommendations/assessments by European cybersecurity bodies regarding Kaspersky

- **FRANCE** – Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
  - "In the current context, the use of certain digital tools, in particular those of the Kaspersky company, may be questioned because of their link with Russia. At this stage, there is no objective reason to change the assessment of the quality of the products and services provided."

- **ITALY** – Agency for National Cybersecurity (ACN)
  - "In this regard, to date, there is **no objective evidence** of a decline in the quality of the technological products and services provided."

- **SWITZERLAND** – National Cyber Security Center (NCSC)
  - "To date, **no misuse of the Kaspersky anti-virus software** in Switzerland has been reported to the NCSC. If the NCSC receives verified information about misuse, the public will be informed and warned immediately."

Other recommendations/assessments by European cybersecurity bodies regarding Kaspersky

- **UNITED KINGDOM** – National Cyber Security Centre (NCSC)
  - "We've had enquiries from people worried about their home IT. It almost certainly remains the case that nearly all individuals in the UK (and many enterprises) are not going to be targeted by Russian cyber attack, **regardless of whether they use Russian products and services."**

- **NETHERLANDS** - National Cyber Security Center (NCSC) and Digital Trust Center (DTC)
  - "There is currently no reason to suspect that there is an increased risk for companies in the use of Kaspersky software."

- **BELGIUM** – Centre for Cybersecurity Belgium (CCB)
  - "[Also] the Centre for Cybersecurity Belgium (CCB) sees no threat at the moment."

Other recommendations/assessments by European cybersecurity bodies regarding Kaspersky

- **AUSTRIA** – Austrian Cert (CERT.at)
  - "CERT.at currently has no information that Kaspersky products contain malicious functions."

- **HUNGARY** - National Cyber Defence Institute (NSSNKI)
  - "The NBSZ NKI does not recommend [to its customers, ie Hungarian government administration and local municipalities] the use of Kaspersky Lab products"

- **LUXEMBOURG** – Computer Incident Response Center (CIRCL.lu)
  - "In our opinion and while expecting more tension in the conflict, it would be a move to consider to temporarily suspend the usage of this product and replace it with something else, for instance Windows Defender (to give an option without additional cost)."

kaspersky

Kaspersky‘s Group structure and principles

What sets Kaspersky apart!

Global supplier – key market Europe – holding UK

Active in ca. **200** countries and territories

34 representative regional offices

North America
Mexico
USA

South America
Brazil
Argentina
Columbia
Mexico

Africa
South Africa

Australia

Europe
Austria
Czech Republic
Denmark
France
Germany
Israel
Italy
Netherlands
Poland
Portugal
Romania
Russia
Spain
Switzerland
UK (Holding)

Asia
China
Hong Kong
India
Japan
Kazakhstan
Malaysia
Singapore
South Korea
Turkey
UAE

Transparency Centers
Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia
New Brunswick, Canada

Structure of the Kaspersky group

- **The parent company (holding company) is Kaspersky Labs Limited (KLL),** headquartered in **London, UK.**
- **Both the holding company and the subsidiaries** (including those in Germany, France, Italy, Austria, Russia, Spain, Switzerland, Romania, the USA, China and many other countries) **are limited liability companies**

*Official information on the holding company **KLL** and the British subsidiary **Kaspersky Labs UK Limited** (KLUK), including tax reports, can be found on the website of the British Trade Register:*

- KLL - https://find-and-update.company-information.service.gov.uk/company/04249748
- KLUK - https://find-and-update.company-information.service.gov.uk/company/03654151

Research & development

>4,300 highly qualified specialists

1/3 R&D specialists

40+ world-leading security experts, our elite group GReAT

> 400.000.000 private users

> 240.000 business clients

Our contribution to cyber-resilience in Europe

Kaspersky works closely together with **international organizations as well as public institutions and private stakeholders** to ensure the security and safety of European citizens.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Industry partner of the Council of Europe Human Rights Organization to promote respect for human rights, democracy, and the rule of law on the Internet.

enisa
THE EU CYBERSECURITY AGENCY

Member of the AHWG on EU Threat Landscape and contributor to publications like the study *"Good Practices for Security of IoT - Secure Software Development Lifecycle"*

PARIS 11 · 12 CALL

Supporter of the Paris Call to address cybersecurity issues through global collaboration

Horizon 2020 Programme

Kaspersky currently takes part in four HORIZON 2020 consortiums: CitySCAPE, IoTAC, GEIGER, and TRAPEZE

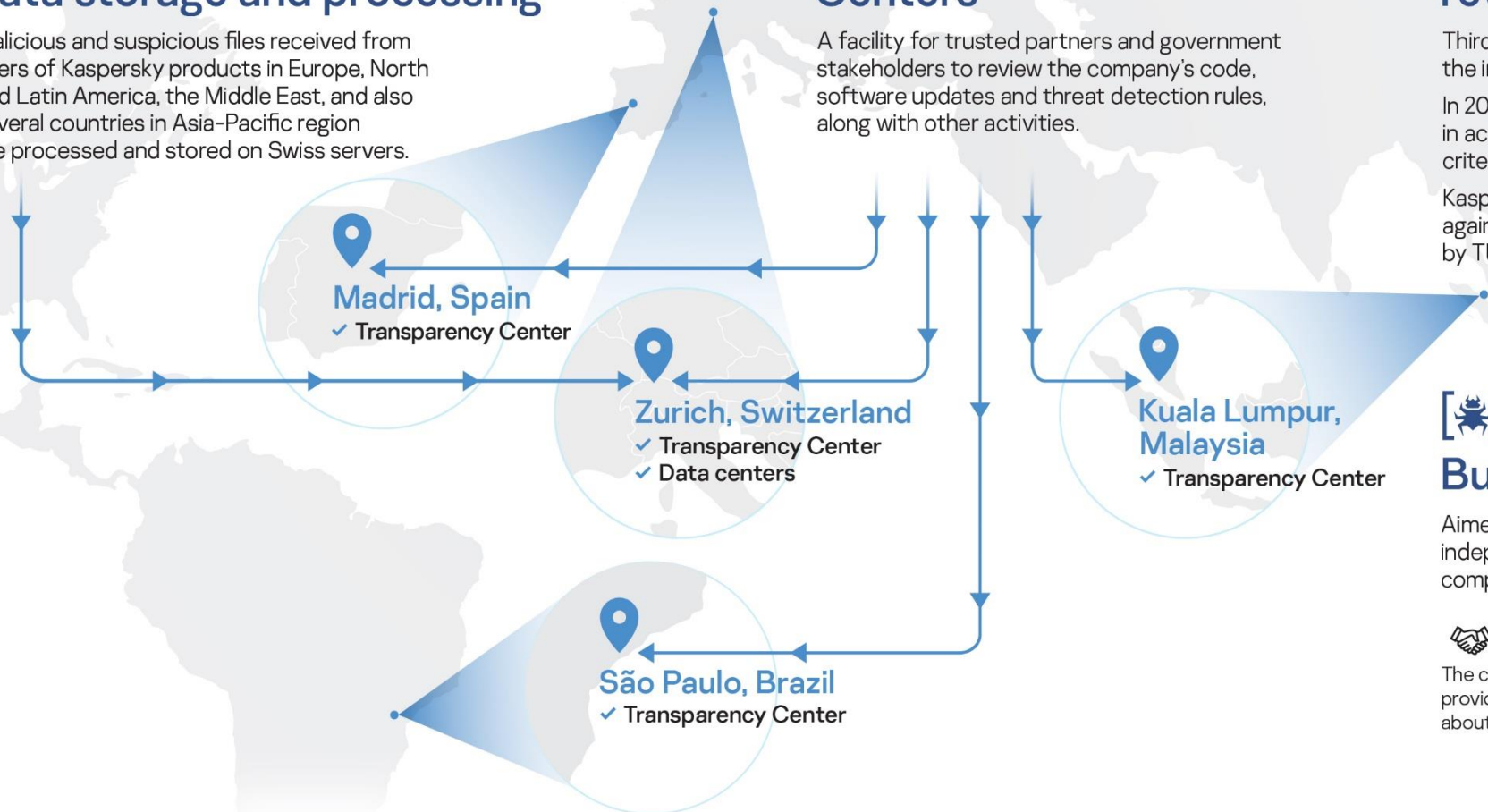
Kaspersky Global Transparency Initiative

Cyberthreat-related user data storage and processing

Malicious and suspicious files received from users of Kaspersky products in Europe, North and Latin America, the Middle East, and also several countries in Asia-Pacific region are processed and stored on Swiss servers.

Transparency Centers

A facility for trusted partners and government stakeholders to review the company's code, software updates and threat detection rules, along with other activities.



Independent review

Third-party assessment of internal processes to verify the integrity of Kaspersky solutions and processes.

In 2019 Kaspersky has achieved the SOC 2 Type 1 report in accordance with the SSAE 18 standard (Security criteria) issued by one of the Big Four accounting firms.

Kaspersky's data services have also been certified against ISO/IEC 27001:2013 international standard by TÜV AUSTRIA.

Bug bounty program

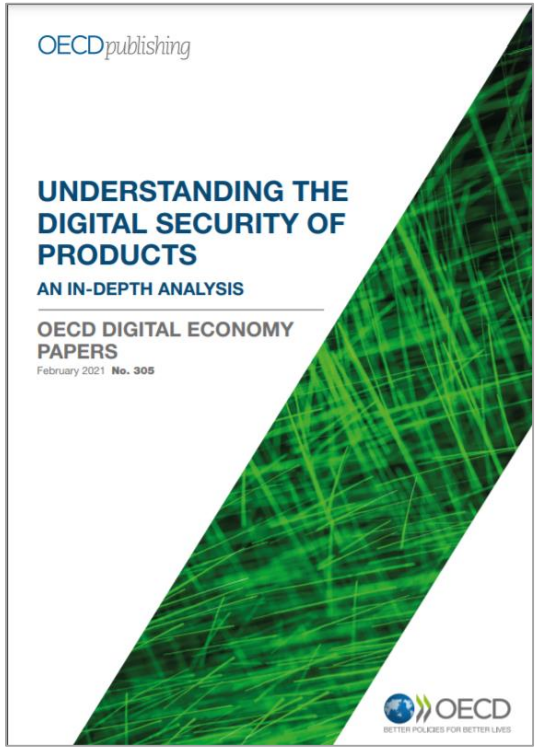
Aimed to make Kaspersky more secure, it encourages independent security researchers to supplement the company's own work in vulnerability detection and mitigation.

The company also supports the Disclose.io framework which provides Safe Harbor for vulnerability researchers concerned about possible negative legal consequences of their discoveries.

kaspersky BRING ON THE FUTURE

Proven. Transparent. Independent.

International publications to which Kaspersky has contributed



International collaboration, transparency, trust, risk management and local responsibility: five pillars of Kaspersky's DNA

Why you can trust Kasperky, even with the geopolitical situation and the motivated warning by the BSI

kaspersky

kaspersky

Appendix:
The geopolitical **BSI warning!**

In our opinion, the BSI warning is illegal because the BSI law does not provide a basis for a geopolitical warning!

BSI law

Section 7 warnings

(1) In order to perform its duties pursuant to section 3 (1) sentence 2 numbers 14 and 14a, the Federal Office may

1. issue the following warnings and information to the public or affected parties:

(a) warnings about security vulnerabilities in information technology products and services,

(b) warnings about malicious programs,

(c) warnings about loss of or unauthorized access to data; and

(d) information about security-related IT features of products.

2. recommend security measures and the use of specific security products.

In our opinion, the BSI warning is illegal because the BSI law does not provide for a geopolitical warning!

BSI law

§7 warning

(2) In order to fulfill its tasks pursuant to Section 3 (1), sentence 2, numbers 14 and 14a, the Federal Office may warn the public of security vulnerabilities in information technology products and services and of malicious programs, stating the name and manufacturer of the product and service concerned, if there are sufficient indications that they pose a threat to information technology security, or recommend security measures and the use of certain information technology products and services. If the information provided to the public subsequently turns out to be incorrect or the underlying circumstances to have been misrepresented, this must be made public without delay.

In our opinion, the BSI warning is illegal because the BSI law does not provide for a geopolitical warning!

BSI law

§3 Tasks of the federal office

(1) The Federal Office shall promote security in information technology with the aim of ensuring the availability, integrity, and confidentiality of information and its processing. To this end, it shall perform the following important tasks in the public interest:

(...)

(...)14. advising, informing and warning federal and state agencies, as well as manufacturers, distributors and users, on issues relating to security in information technology, in particular taking into account the possible consequences of a lack of or inadequate security precautions;

14a. Consumer protection and consumer information in the area of security in information technology, in particular by advising and warning consumers in matters of security in information technology and taking into account the possible consequences of missing or insufficient security precautions;

The BSI is warning against a flawlessly functioning antivirus software!

The term **security vulnerability** is defined in **Section 2 (6) BSI-Act**. According to this, security vulnerabilities are:

"Properties of programs or other information technology systems, the exploitation of which makes it possible for third parties to gain access to third-party information technology systems against the will of the authorized party or to influence the function of the information technology systems."

The explanatory memorandum to the law states:

"Security vulnerabilities, on the other hand, are undesirable characteristics of information technology systems, especially computer programs, that allow third parties to influence their information technology against the will of the authorized party."

Cf. Bundestags-Drucksache 16/11967, S. 12. - 4 - 6. April 2022 14/14-22.146

It is clear from the wording of the definition that a security vulnerability **only exists when the program itself is affected and when undesirable properties of information technology systems, in particular computer programs, are involved.**

Incomprehensible interpretation of the term "security vulnerability”

- *the court assumes that **antivirus software** is, **by definition, a security vulnerability**.*
- *The court believes that these **security vulnerabilities are acceptable if the manufacturer is particularly trustworthy**.*
- *However, if the **manufacturer is no(t) (longer) trustworthy, it is a security vulnerability**.*