kaspersky

International cooperation, transparency, trust, risk management, and local responsibility: Five important pillars of Kaspersky's DNA

As a global cybersecurity company, Kaspersky contributes significantly to cybersecurity and resilience in Europe and around the world. Kaspersky is a privately held group of companies. The group's holding company is Kaspersky Labs Limited (KLL). It is registered in London, the UK. There are 13 legally independent Kaspersky national companies operating in various countries of Europe. These companies are all subsidiaries of KLL. All Kaspersky national companies pay their taxes, salaries and social security contributions in Europe. The company also conducts research and development in Europe. Its Global Research and Analysis Team (GReAT) is managed from Bucharest, Romania. Most of the global GreAT team is based in Europe.

This paper provides information on the following:

- How Kaspersky increases user protection and security through national as well as cross-border and cross-industry collaboration;
- Why strengthening cybersecurity and increasing cyber resilience drives our actions;
- Why Kaspersky considers transparency and trust to be the essential foundations for secure digitization.

Kaspersky's work is driven and motivated by the need of citizens, businesses, and governments in Europe and around the world to take advantage of the opportunities of digitalization in a secure, reliable, and trustworthy manner.

1/ Resilient, secure, transparent business processes

Kaspersky's business processes are designed for **maximum resilience**, so that customers and partners can rely on the **best possible business continuity** even in times of geopolitical tension. This is made possible by a balanced and structured distribution of tasks and responsibilities between HQ and the national subsidiaries, by **organizational**, **infrastructural** and **technical measures**, as well as comprehensive and goal-orientated **employee qualifications**. This enables us to ensure that we meet our obligations to partners, customers and potential new customers in the best possible way - from supplying products and providing support to securing financial transactions.

2/ Cooperation at European level

The European single market is the largest cybersecurity market in the world. This is also true for Kaspersky: Europe is the largest market for the company - across all industries. Therefore, Europe is central to Kaspersky's corporate strategy. Here, we collaborate with numerous national and international organizations. For example, we are involved in several studies and publications of the **European Union Agency for Cybersecurity, ENISA**. A researcher from our GReAT team is a member of the ENISA ad hoc working group on "EU Cyber Threat Landscapes." Together with Europol, the Dutch police, and McAfee, we also launched the **NoMoreRansom** global initiative. We are currently a consortium partner in four **European Horizon 2020** projects. Together with ENISA and the German Federal Office for Information Security (BSI), our experts contributed to a consultation on AI and cybersecurity of the European Parliament's AIDA Committee in January 2021.

kaspersky

3 / Global cooperation

Kaspersky is an industry partner of the **Council of Europe** to promote an open and secure internet, and is a partner of the **Geneva Dialogue on Responsible Behavior in Cyberspace**. Kaspersky has contributed to the **OECD 2021 reports** on digital security and vulnerability management, is one of the first signatories of the Paris Call for Trust & Security in Cyberspace, and participates in **United Nations discussion forums** such as the **UN Open Working Group on Information and Communication Technology Developments in the Context of International Security**, and contributes to the **Internet Governance Forum (IGF)**. We are involved in all these bodies and organizations because trustworthy cooperation and information sharing are essential in cybersecurity. Kaspersky is valued as a trusted partner in Europe and worldwide.

4 / Diversified financial system

Kaspersky has operated a diversified financial system since 2008. The national companies manage their finances independently – from the independent handling of income and expenses to the handling of partner orders. The country units conduct their financial transactions in their respective countries and use local banks.

5 / Global Transparency Initiative (GTI)

As part of the Global Transparency Initiative (GTI), Kaspersky has taken the following measures:

- Data storage and processing are located in Switzerland. Kaspersky operates a data infrastructure in two highly secure data centers in Zurich to process and store cyberthreat data from customers in Europe, the United States, and Canada, as well as several Asia-Pacific countries.
- Establishing "transparency centers" for reviewing source code, all versions of our builds and AV database, software development, and data management – including reviewing the information Kaspersky products send to the cloud-based Kaspersky Security Network (KSN). Kaspersky also provides access to its source code to ensure it matches publicly available modules. Kaspersky also provides the software bills of materials (SBOM) for its products. The transparency centers are located in Zurich, Madrid, Kuala Lumpur, and São Paulo.
- The security and reliability of our technical and organizational procedures and data services have been confirmed by two external, independent audit organizations. Kaspersky successfully passed in 2019 and again in 2022 the SOC-2 (Service Organization Control for Service Organizations) Type 1 audit by a Big Four auditor, which confirmed the security of Kaspersky's process for developing and releasing AV updates against the risk of unauthorized changes. In addition, our data services were certified according to ISO/IEC 27001:2013.
- Organizing our Vulnerability Management Program. In March 2018, as part of our bug bounty program, Kaspersky increased the bounties for external researchers who find critical vulnerabilities in the company's products up to $100,000. Since then, Kaspersky has awarded 53 bounties even though no critical vulnerability has ever been reported. With this approach to vulnerability analysis, management and disclosure, Kaspersky is constantly improving the security of its products. To create more transparency in vulnerability management, Kaspersky has published ethical principles for responsible vulnerability disclosure.