



Constantin Moldovan <constantin.moldovan@publicrecord.ro>

Request for comment: Kaspersky products used by Romanian public institutions

Darko Natalic <Darko.Natalic@kaspersky.com>

mie., 14 oct., 13:53

Către: constantin.moldovan@publicrecord.ro <constantin.moldovan@publicrecord.ro>

Dear Mr. Moldovan,

Thank you for your interest and the inquiry.

Kaspersky is a private, global business focused on its mission to protect its customers around the world from cyberthreats and build a safer world. As a company focused on serving the security needs of individuals, companies and governments all around the world, Kaspersky does not have any inappropriate ties to any government.

Acknowledging that the work of any cybersecurity solution requires deep system access, Kaspersky has always advocated for the development of a cybersecurity assessment methodology relying on technical evidence. For our part, we have introduced a number of practices, enabling the company's stakeholders to check and verify the security and trustworthiness of our solutions and ascertain the sustainability of our supply chain as part of our Global Transparency Initiative, spanning source code reviews to a bug bounty program. Beyond that, the security and integrity of the company's data services and engineering practices have been confirmed by independent third-party assessments, including through the SOC 2 Audit and ISO/IEC 27001:2022 certification.

Kaspersky has maintained that the claims about alleged security risks that the company's products might have and related restrictions are based on the current geopolitical climate rather than a technical analysis of Kaspersky software security. To date, no party has presented any public evidence that the company's products might pose a threat to corporate or private users.

Kaspersky is always prepared to address any concerns that regulators and customers may have regarding our operations and products in a fully transparent, open, and objective manner, including through Kaspersky Transparency Centers operating in Europe.

Kind regards,

Darko Natalić | Corporate Communications Manager Eastern Europe | Kaspersky

Mobile: +381 64 642 8035 | darko.natalic@kaspersky.com

www.kaspersky.com | <https://www.kaspersky.com/blog/>

From: Constantin Moldovan <constantin.moldovan@publicrecord.ro>

Sent: Monday, October 12, 2026 3:08 PM

To: PRHQ <prhq@kaspersky.com>

Subject: Re: Request for comment: Kaspersky products used by Romanian public institutions

Caution: This is an external email.

I'm following up on my previous request regarding the purchase and use of Kaspersky products by Romanian public institutions. We would still appreciate Kaspersky's response. The story is scheduled for publication on **Friday, October 16**. We would appreciate a response by **Wednesday, October 14, at 12:00 PM Romanian time**, so we can include Kaspersky's position in the article.

On Sat, Oct 3, 2026 at 7:47 PM Constantin Moldovan <constantin.moldovan@publicrecord.ro> wrote:

Dear Kaspersky HQ Communications Te-am,

- My name is [Constantin Moldovan](#) and I am contacting you on behalf of Public Record from Romania, regarding a story related to Kaspersky products used by Romanian public institutions and would like to request an official statement or response from Kaspersky regarding our findings.

1.

In 2022, amid the war in Ukraine, the Romanian Parliament passed cybersecurity legislation banning public sector entities from acquiring or utilizing software produced or controlled

by Russian entities. The list of banned products was published in March 2023 and explicitly targets a wide range of Kaspersky products. The government stated that the presence of Russian antivirus software is "a vulnerability to the cybersecurity" of Romanian

institutions. What is Kaspersky's position on these restrictions, and how do you respond to the characterization of your software as a security risk?

2. The U.S. Department of Commerce has argued that, because Kaspersky is subject to Russian jurisdiction, the Russian government could compel the company to provide information or assistance, including cooperation with intelligence services.

Can Kaspersky explain what legal safeguards, if any, would allow it to refuse a request from Russian authorities for access to customer information, telemetry, software infrastructure or update mechanisms?

Has Kaspersky ever received a request from a Russian government agency or intelligence service to provide customer data, technical access or assistance? If so, can the company disclose how it responded?

3. Given that regulatory bodies in Germany and the U.S. have flagged the high-level system permissions and software update capabilities of antivirus solutions as potential security risks, what is Kaspersky's official position on these assessments, and how do you guarantee user privacy and system security under such privileges?

4. In 2017, a Kaspersky software installed on the computer of a U.S. government contractor uploaded files containing material related to the NSA to Kaspersky's systems. Kaspersky has previously said this happened automatically as part of malware detection.

What changes, if any, has the company made since then to prevent legitimate sensitive or classified files from

being uploaded through automated security processes?

5. In 2019, a German journalist revealed a feature in Kaspersky antivirus products that could potentially be used to track users across websites. According to a blog post, Kaspersky stated that the “bug” was fixed. How do you reassure your users that local traffic interception tools do not compromise end-user privacy or open secondary security vulnerabilities?

6. Kaspersky has repeatedly stated that it is a private company independent of the Russian government. Could you explain what corporate governance, ownership and technical safeguards ensure this independence in practice?

[Text citat ascuns]