

EN

E-001941/2026

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(3.7.2026)

In the present geopolitical context, the Commission is a high-profile target for cyberattacks. Their scenarios are increasingly complex and deceptive, as threat actors use more advanced techniques, including artificial intelligence. This trend is demonstrated by the two recent significant incidents. Neither of them caused any major disruption to the Commission's IT systems, proving that cybersecurity measures put in place by the Commission in line with Regulation 2023/2841¹ – and continuously improved in cooperation with CERT-EU² – are effective in detecting and containing the attack attempts swiftly, and in reducing their impact. A thorough investigation of the personal data breach dimension of both incidents was conducted, in full respect of the regulatory obligations.

The incident involving the cloud infrastructure of the europa.eu platform points to a major and growing risk of software supply-chain attacks. The Commission is reinforcing the measures aiming at verification of software origin and authenticity, tighter controls on third-party and open-source components, continuous monitoring, and defence-in-depth to limit the propagation of attacks. Lessons learned from all incidents are systematically used to improve the Commission's internal operational protocols. Besides, the Commission proposed a new framework to strengthen the security of information and communications technologies supply chains in the revised Cybersecurity Act 2³.

The roles and responsibilities in cybersecurity in the Commission are defined in the internal cybersecurity risk-management, governance and control framework⁴, in full compliance with the provisions of Regulation 2023/2841, in particular with regards to reporting obligations.

¹ Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, OJ L, 2023/2841, 18.12.2023.

² The Cybersecurity Service for the Union institutions, bodies, offices and agencies.

³ Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2), COM/2026/11 final.

⁴ Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, C/2016/8998.