

EN

E-002452/2026

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(7.9.2026)

The Cyber Resilience Act¹ (CRA) establishes essential cybersecurity requirements for products with digital elements, including mobile phones, operating systems and mobile applications, aimed at strengthening protection from cyber threats for users of such products.

In order to support the implementation of the CRA, the Commission requested to the European standardisation organisations the development of a number of harmonised standards², including one for operating systems³. The EU Agency for Cybersecurity (ENISA) is also supporting the implementation of the CRA through a range of technical guidance documents for manufacturers⁴.

Furthermore, the CRA establishes obligations for distributors, including the need to act with due care in relation to the requirements of the Regulation and to withdraw and recall, if appropriate, products with digital elements that are not in conformity with the essential cybersecurity requirements set out in the CRA.

In addition, the NIS2 Directive⁵ requires providers of public electronic communication networks and of publicly available electronic communication services to take cybersecurity risk management measures to protect their services. More recently, the trusted information and communication technologies (ICT) supply chain framework in the revised Cybersecurity Act⁶ proposes measures to ensure the security of the ICT supply chain of electronic communications networks and protect them from strategic cybersecurity risks notably linked with high-risk suppliers.

Finally, the ePrivacy Directive⁷ protects the integrity of mobile endpoints by making access to such endpoints and the processing of information stored on such endpoints in principle subject to consent of the user.

¹ Regulation (EU) 2024/2847.

² C(2025) 618 final.

³ Products with digital elements that have the core functionality of operating systems will need to apply that harmonised standard or be subject to a more stringent conformity assessment procedure, in accordance with Article 32(2).

⁴ ENISA Secure by Design and Default Playbook <https://www.enisa.europa.eu/publications/enisa-secure-by-design-and-default-playbook> or

ENISA Technical Advisory for Secure Use of Package Managers

<https://www.enisa.europa.eu/publications/enisa-technical-advisory-for-secure-use-of-package-managers>.

⁵ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

⁶ COM(2026) 11 final.

⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).