

EN

E-000997/2025

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(13.6.2025)

The Interoperable Europe Act¹ mandates EU and public bodies to conduct interoperability assessments (since 2025) and promotes cross-border collaboration via a share-and-reuse mechanism for solutions. This addresses interoperability gaps in states like Romania. To strengthen cybersecurity, the EU equipped itself with an extensive and solid legal framework, which includes the NIS2 Directive², the Cyber Resilience Act³, the Cyber Solidarity Act⁴ and the Cybersecurity Act⁵ establishing the European Union Agency for Cybersecurity (ENISA), while the Digital Europe Programme (DEP) and Recovery and Resilience Facility (RRF) fund IT infrastructure upgrades. For example, the Romanian recovery and resilience plan contains several reforms and investments to bolster cybersecurity of public and private entities for a budget of approximately EUR 138 million.

The European Digital Identity (EUDI) Wallet and upcoming EU Business Wallet provide secure, harmonised digital identification for citizens, businesses, and public administrations to authenticate, receive notifications, and share verified credentials.

For data protection, the Once-Only Technical System (OOTS) enables secure cross-border data sharing (e.g. birth certificates), identification through eIDAS/EUDI Wallets, with user consent and data previews.

The Digital-Ready Policymaking (DRPM) framework ensures EU policies embed interoperability safeguards, including a mandatory ‘digital statement’ during policy design.

Together, these initiatives streamline access to digital services (e.g. a Romanian citizen sharing data with a German institution) while ensuring compliance with the General Data Protection Regulation (GDPR)⁶ and cybersecurity standards.

¹ Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union; OJ L, 2024/903, 22.3.2024.

² 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; OJ L 333, 27.12.2022, p. 80–152.

³ Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828; OJ L, 2024/2847, 20.11.2024.

⁴ Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694; OJ L, 2025/38, 15.1.2025.

⁵ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013; OJ L 151, 7.6.2019, p. 15–69.

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; OJ L 119, 4.5.2016, p. 1–88.