

EN

E-004766/2025

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(9.2.2026)

Directive (EU) 2022/2555¹ aims to increase the cybersecurity of entities operating in eighteen critical sectors, including public administration. Under this Directive, Member States must ensure that certain public administration entities have to take cybersecurity risk-management measures, including concerning security in network and information systems acquisition and supply chain security.

Further, Directive (EU) 2022/2555 requires Member States to adopt a national cybersecurity strategy which must contain policies on the inclusion and specification of cybersecurity-related requirements for information and communications technology products and services in public procurement.

Assuming that the award procedure referred to is subject to Directive 2014/24/EU², the Commission considers that national courts and review bodies laid down under the Directives on remedies in public procurement³ are in the best position to assess, according to the facts of each case, whether contracting authorities and contracting entities have respected their obligations under EU law.

¹ 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 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

² Directive (EU) 2014/24 of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, pp. 65–242).

³ In the case at hand, Council Directive (EEC) 89/665 of 21 December 1989 on the coordination of the laws, regulations and administrative provisions relating to the application of review procedures to the award of public supply and public works contracts (OJ L 395 30.12.1989, p. 33).