(English version)

Question for written answer E-002458/24
to the Commission
Beatrice Timgren (ECR), Charlie Weimers (ECR), Dick Erixon (ECR)
(7 November 2024)

Subject: Impact of new cybersecurity regulations on SMEs in digital services

The recent Directive (EU) 2022/2555 ([1]) on cybersecurity, introduced by the Commission, establishes broad requirements for companies in online services — including DNS providers, cloud services, online marketplaces and social networking platforms — with specific stipulations for risk management, incident reporting and supply chain security. While these measures aim to strengthen network security across the EU, they pose significant financial and operational challenges, particularly for the small and medium-sized enterprises (SMEs) and micro-entities which are prevalent in the digital sector.

1. Given the high compliance costs and complex requirements detailed in the directive, what steps is the Commission considering to alleviate the regulatory and financial burdens on SMEs in the digital sector?

2. Does the Commission plan to provide specific resources or guidance tailored to help smaller firms fulfil these cybersecurity standards without undermining their operational viability and competitiveness in the global market?

Submitted: 7.11.2024

Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(10 January 2025)

Directive (EU) 2022/2555 (NIS2) ([1]) applies, with some exceptions such as for telecom providers or domain name system (DNS) service providers, in principle to medium-sized or larger entities in 18 sectors, which are critical for the EU economy and society.

It follows a risk-based approach requiring entities to take appropriate and proportionate cybersecurity risk management measures depending on the risks they face.

In addition to the recently adopted Implementing Regulation (EU) 2024/2690 ([2]), which specifies the requirements for cybersecurity measures and defines the thresholds for a significant incident for various categories of digital services and providers, the European Union Agency for Cybersecurity (ENISA) is now consulting stakeholders ([3]) on a guidance document further explaining these requirements.

Both will help small and medium-sized enterprises (SMEs), as they offer additional guidance on the implementation of NIS2 and advance harmonisation across the EU.

Moreover, the EU is funding SMEs by Horizon Europe ([4]) (cluster 3) and Digital Europe Programme (DEP) ([5]). DEP has been explicitly supporting the uptake of EU cyber legislations by SMEs and promoting their competitiveness since 2022. It gave EUR 70 million from 2022 to 2024, and in addition it will devote around EUR 30 million up to 2027.

Furthermore, Regulation (EU) 2024/2847 ([6]) (Cyber Resilience Act, CRA) includes provisions on dedicated support measures for microenterprises and SMEs.

In 2024, the EU allocated EUR 30 million to develop guidance and compliance tools (including automatic compliance tools) for SMEs.

This will help them to comply with the CRA, which in itself would support them in meeting the NIS2 supply chain security requirements.

---

1 [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, OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

([1]) http://data.europa.eu/eli/dir/2022/2555/oj

([2]) http://data.europa.eu/eli/reg_impl/2024/2690/oj

([3]) https://ec.europa.eu/eusurvey/runner/ENISA_Guide_Feedback_Form

([4]) https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en

([5]) https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital

([6]) http://data.europa.eu/eli/reg/2024/2847/oj