

(English version)

**Question for written answer E-001462/25
to the Commission
Morten Løkkegaard (Renew)
(9 April 2025)**

Subject: Possibilities of strengthening data security within public procurement regulation

In a rapidly changing world, it is paramount that we do not treat our data security lightly, as we risk exposing our citizens and societies to data-driven threats and surveillance from malign actors. Therefore, we need to strengthen the awareness and legislative framework in this regard, especially concerning the public procurement of data-heavy products such as electric vehicles, drones and the like. Can the Commission, in this regard:

1. Confirm that using ‘data security’ as a procurement criterion on a par with economic and environmental criteria is permitted within the current Public Procurement Directive?
2. Outline what proposals the Commission envisages to put forward to further strengthen data security with the forthcoming revision of the Public Procurement Directive?
3. Outline any further proposals the Commission plans to put forward, in order to strengthen the data security of citizens and societies alike?

Submitted: 9.4.2025

**Answer given by Executive Vice-President Séjourné on behalf of the European Commission
(14 July 2025)**

The Commission confirms that ‘data security’ can be used in public procurement as a technical specifications requirement or as part of the awarding criteria.

It is up to the public buyers to define the adequate procurement solution that meets their specific needs and reflect it adequately in the tender documents.

The evaluation of the EU public procurement framework is ongoing. Security aspects, including data security, are discussed in this context.

Once the evaluation is concluded, its outcome will be taken into account in the impact assessment of the forthcoming revision. As a principle, public procurement regulates only the process of purchasing. Public buyers have already various ways to include security aspects in their tenders.

From the general cybersecurity perspective, the Commission is monitoring the current transposition of the Network and Information Systems (NIS2) Directive ⁽¹⁾ which requires entities from 18 critical sectors to take organisational cybersecurity risk-management measures to protect their network and information systems, which include the digital data stored, processed, retrieved or transmitted.

The Commission is also monitoring and supporting the implementation of the Cyber Resilience Act ⁽²⁾, which ensures, among others, cybersecurity by design (including protection of processed data) of products with digital elements placed on the EU market as of 11 December 2027.

⁽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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

⁽²⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02024R2847-20241120>.