

(English version)

**Question for written answer E-001813/26
to the Commission
Jaume Asens Llodrà (Verts/ALE)
(4 May 2026)**

Subject: Use of data analytics software in security and defence: compliance with EU law and fundamental rights

According to recent reports, several Member States have awarded contracts to companies such as Palantir Technologies for the use of large-scale data analytics software in the fields of security and defence, in some cases through procedures that lack transparency. These technologies raise concerns regarding the protection of personal data and may create situations of technological dependency on external providers.

1. Does the Commission have information on these contracts, and has it assessed their compliance with Regulation (EU) 2016/679 and Directive (EU) 2016/680, particularly with regard to proportionality, purpose limitation and international data transfers?
2. Does the Commission intend to adopt measures or guidelines to ensure that the public procurement of artificial intelligence technologies in the field of security fully respects fundamental rights, transparency and the EU's technological sovereignty?

Submitted: 4.5.2026

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(16 September 2026)**

EU data protection law, including Regulation (EU) 2016/679 ⁽¹⁾ and Directive 2016/680 ⁽²⁾, sets out the principles and rules to be complied with for the processing of personal data, regardless of the technology used.

The enforcement of those rules lies primarily with national data protection supervisory authorities and courts. The EU data protection law does not apply in case of state activities with genuine national security or defence purposes.

The AI Act ⁽³⁾ establishes harmonised EU rules for trustworthy AI, but it does not apply to AI systems used exclusively for military, defence, or national security purposes.

Where AI systems are also used for other purposes (e.g. law enforcement), the AI Act applies ⁽⁴⁾, and such systems may be classified as high-risk under the AI Act rules or fall under the prohibitions laid down in Article 5 (e.g. social scoring and predictive policing).

For AI systems covered by the AI Act, Article 62(3)(d) requires the AI Office to evaluate and promote the convergence of best practices in public procurement procedures in relation to such systems.

To support Member States and businesses in tackling cybersecurity risks and harnessing opportunities related to the development of frontier AI models, the Commission has adopted on 7 July 2026 an Action Plan on Cybersecurity and AI that offers a structured, coherent and prioritized framework to bolster the preparedness of the EU ⁽⁵⁾.

⁽¹⁾ <http://data.europa.eu/eli/reg/2016/679/2016-05-04>.

⁽²⁾ <http://data.europa.eu/eli/dir/2016/680/2016-05-04>.

⁽³⁾ <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

⁽⁴⁾ Article 2(3) and Recital 24 of the AI Act.

⁽⁵⁾ <https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence>.