

(English version)

**Question for written answer E-003287/25
to the Commission
Kosma Złotowski (ECR)
(25 August 2025)**

Subject: Security of EU databases in the context of Spain's agreement with Huawei

The Spanish Government has decided to award Huawei a contract worth EUR 12.3 million to manage and store data from judicial wiretaps. This information is used by security services and judicial authorities. Huawei's presence in such a sensitive domain may pose a risk to national security and undermine the trust of other Member States. It is worth recalling that, in 2019, one of Huawei's directors who sold services to public institutions was arrested by the Polish authorities on espionage charges.

Spain claims that the infrastructure is isolated, audited and meets the highest safety requirements. However, both the European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Criminal Justice Cooperation (Eurojust) rely on cooperation from Member States on the basis of information exchanges in tackling crime, including for personal data, making this contract a source of concern. The risk of Chinese intelligence services infiltrating such a database constitutes a significant danger.

1. By signing this contract, is Spain not acting against the EU principle of sincere cooperation by downplaying the security risks that Huawei's presence in such a sensitive domain poses to the security of EU citizens' data?
2. Does the Spanish Government's decision align with the EU's digital sovereignty strategy, created in the context of the expansion of Chinese technology suppliers?
3. Is the Commission monitoring this contract in any way and has it requested clarification from the Spanish Government in view of its possible negative impact on cooperation with Spain within Europol and Eurojust?

Submitted: 25.8.2025

**Answer given by Executive Vice-President Virkkunen on behalf of the European Commission
(19 November 2025)**

In the communication on the implementation of the EU 5G Toolbox ⁽¹⁾, the Commission assessed that Huawei (and ZTE) present materially higher risks than other 5G suppliers.

The Commission has committed to avoiding exposure of its own corporate communications networks to mobile networks using these suppliers and to reflect this decision, in accordance with its competences under the respective governance rules, in all relevant EU funding programmes and instruments.

The Commission also considered that Member States' decisions to restrict or exclude these suppliers from 5G networks are justified and compliant with the 5G Toolbox. It urged all Member States to implement the Toolbox and take measures to mitigate the risks linked to these suppliers.

The concerns surrounding Spain's contract with Huawei, particularly regarding managing and storing judicial wiretaps data, involve key aspects of data protection governed by the Law Enforcement Directive ⁽²⁾ (LED), along with its national transposition.

In particular, Article 4(1) (f) lays down principles relating to processing of personal data, including ensuring appropriate security of personal data processed for law enforcement purposes such as judicial wiretapping.

Article 29 lays down further requirements such as preventing the unauthorised inspection, modification or deletion of stored personal data.

The contract concluded by the Spanish Ministry of the Interior with Huawei can potentially create a dependency on a high-risk supplier in a critical and sensitive sector that would increase the risk of foreign interference. Therefore, adherence to the LED is crucial to preserving data integrity and security.

⁽¹⁾ C(2023) 4049 final.

⁽²⁾ Directive (EU) 2016/680.