

(English version)

**Priority question for written answer P-002371/26
to the Commission**

Helmut Brandstätter (Renew), Lara Wolters (S&D), Elisabeth Grossmann (S&D), Sandro Gozi (Renew), Marta Temido (S&D), Elisabetta Gualmini (Renew), Kim Van Sparrentak (Verts/ALE), Andreas Schieder (S&D), Lukas Sieper (Renew), Mounir Satouri (Verts/ALE)

(9 June 2026)

Subject: Sovereignty of European payment system Wero

At a time when the EU is actively attempting to regain strategic sovereignty, recent media reports indicating that Wero uses servers owned by a foreign company (Amazon Web Services, Inc. (AWS)) raise questions about the safety of European payment systems. ⁽¹⁾

Wero, a growing European alternative to foreign payment system monopolies, claims to have over 50 million active European users, and has access to their most sensitive data.

Multiple countries outside the EU, including the United States, have laws (e.g. the CLOUD Act, the Foreign Intelligence Surveillance Act, the Patriot Act and the International Emergency Economic Powers Act) requiring their companies to transfer sensitive data to the authorities or even sanction individuals if asked to do so.

In the light of the recent push towards European self-reliance:

1. Does the Commission acknowledge the risks related to the fact that EU citizens' private data is being stored on the servers of a foreign company (AWS) that is required to share this data with a non-EU country if asked to do so?
2. Has the Commission started an investigation into the Wero case or been in communication with Wero's leadership to address these risks?
3. Will the Commission extend 'Buy European' enforcement mechanisms to private entities in critical sectors, particularly when it comes to the data privacy of European citizens and tech sovereignty?

Submitted: 9.6.2026

Answer given by Mr McGrath on behalf of the European Commission

(10 September 2026)

Under the General Data Protection Regulation (GDPR), companies may transfer personal data to third countries, if they comply with the conditions of Chapter V.

Cross-border transfers of personal data is possible if the data controller ensures that in the third country the data benefits from a level of protection that is essentially equivalent to the one guaranteed in the EU such as through an adequacy decision, or the use of Standard Contractual Clauses.

This ensures that the processing is subject to similar guarantees in the third country and also take into account the possibilities for third country public authorities to access personal data.

It is the role of the independent supervisory authorities in the Member States to assess whether in the specific case of Wero there have been any violations of the GDPR's rules on international data transfers.

In April this year, the European Payments Initiative (EPI) announced on its website that while Wero currently still relies on services from outside Europe in certain areas, it is currently working to reduce its dependency on non-European suppliers.

The proposal for a Cloud and AI Development Act establishes a risk-based sovereignty framework for the procurement by public authorities of cloud computing services. Private companies may also use the same sovereignty framework.

Under Article 31, in specific circumstances and in consultation with the Member states, the Commission is empowered to require businesses operating in sectors of high criticality to carry this assessment and to mandate risk mitigation measures.

In addition, public authorities are required to include award criteria to evaluate the EU added value of the submitted tenders when procuring innovative cloud computing and AI systems.

¹ <https://netzpolitik.org/2026/uneingeloestes-versprechen-auf-digitale-souveraenitaet-europaeischer-bezahldienst-wero-nutzt-amazon-server/>