

(English version)

**Question for written answer E-001198/25
to the Commission**

**Catherine Griset (Pfe), Christophe Bay (Pfe), Mathilde Androuët (Pfe), Virginie Joron (Pfe), Julie Rechagneux (Pfe),
Valérie Deloge (Pfe), Pierre Pimpie (Pfe), André Rougé (Pfe), Pascale Piera (Pfe), Julien Leonardelli (Pfe), Fabrice
Leggeri (Pfe), Aleksandar Nikolic (Pfe)**
(20 March 2025)

Subject: A cloud to call our own!

Under the US' Foreign Intelligence Surveillance Act, American companies have to hand over the personal and professional data of their European clients to American intelligence agencies.

Yet, the EU has concluded an agreement with the US for the transfer of our data called the Data Privacy Framework.

Recently, Democratic members of the Privacy and Civil Liberties Oversight Board, tasked with monitoring that framework in the US, have been dismissed.

Their dismissal is to be welcomed, given the American left's scant regard for civil liberties. However, the new US administration could also order that particular European data be seized.

We must, therefore, be able to store our own personal data, along with that of our administrations and of businesses in the EU, on European cloud hosts.

1. What action is the Commission taking to ease the way for the development of European cloud hosts?
2. Could their development be sped up to replace US solutions if the Court of Justice of the European Union were to annul the Data Privacy Framework?

Supporter ⁽¹⁾

Submitted: 20.3.2025

Answer given by Mr McGrath on behalf of the European Commission
(13 June 2025)

The Commission aims to support an enhanced availability and uptake of European cloud solutions across the EU through the upcoming Cloud and Artificial intelligence Development Act ().

The main objective is to at least triple the EU's overall data centre capacity within the next five to seven years ⁽¹⁾ and ensure that highly critical use cases in the EU are served by highly secure EU-based cloud capacity ⁽²⁾.

The Act will be complemented by a single EU-wide cloud policy for public administrations and public procurement ⁽³⁾.

¹ ⁽¹⁾This question is supported by a Member other than the authors: Jean-Paul Garraud (Pfe)

Mission letter from the President of the European Commission to the Executive Vice-President-designate for Tech Sovereignty, Security and Democracy:
https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf.

⁽¹⁾ This will be achieved by streamlining the permitting procedures and improving access to suitable sites, energy and funding for data centres that meet ambitious resource efficiency requirements. This is an important opportunity for European data centre operators and cloud service providers will have an important role to play in meeting this objective.

⁽²⁾ Such highly critical uses cases in the EU are characterised by high sovereignty and operational autonomy requirements.

⁽³⁾ The aim will be to assist the Act's implementation in the public sector, guide public authorities in their cloud procurement decisions and empower them to leverage their purchasing power more strategically.

Moreover, the Commission has approved the ongoing implementation of the Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services ⁽⁴⁾.

Also, through the co-financing under the Digital Europe Programme, the Commission also supports the deployment of an EU marketplace for federated cloud services ⁽⁵⁾ to facilitate the provision and the procurement of cloud services across the EU by EU cloud service providers ⁽⁶⁾.

The Commission's adequacy decision on the EU-US Data Privacy Framework ⁽⁷⁾ is based on the key safeguards included in Executive Order 14086 (EO 14086) adopted by the President of the United States ⁽⁸⁾.

In particular, EO 14086 introduced safeguards to ensure that the collection and use of personal data of Europeans by United States intelligence agencies is limited to what is necessary and proportionate in pursuit of defined national security objectives.

Moreover, EO 14086 established the Data Protection Review Court, providing EU citizens with a redress mechanism with binding investigatory and remedial powers.

EO 14086 continues to be in place, providing key safeguards to data transferred from the EU ⁽⁹⁾, and addressing all the points raised by the Court of Justice in its Schrems II judgment ⁽¹⁰⁾.

⁽⁴⁾ IPCEI CIS/8ra Europe's Next Generation Cloud Infrastructure and Services — 8ra: <https://www.8ra.com/> Seven Member States will provide up to EUR 1.2 billion in public funding, expected to unlock an additional EUR 1.4 billion.

⁽⁵⁾ Project DOME DOME Mark etplace: https://dome-marketplace.eu/dashboard_

⁽⁶⁾ Such providers offer highly trustworthy, curated cloud services that serve the interests of crucial sectors dealing with sensitive data, such as the public sector.

⁽⁷⁾ Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745) (Text with EEA relevance) C/2023/4745 OJ L 231, 20.9.2023, p. 118-229 https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

⁽⁸⁾ Executive Order 14086 on 'Enhancing Safeguards for United States Signals Intelligence Activities'.

⁽⁹⁾ Its requirements and safeguards have also been recently assessed in the Commission's report of 9 October 2024 to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework COM(2024) 451 final: https://commission.europa.eu/document/25695177-8073-4ce3-bf81-eb816dc6b468_en.

⁽¹⁰⁾ C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), 16 July 2020, ECLI:EU:C:2020:559.