

To Ursula von der Leyen, President of the European Commission
To Michael Michael McGrath, EU Commissioner for Democracy, Justice,
the Rule of Law and Consumer Protection

The credibility of the EU's adequacy framework depends on action, not assumption

Dear President von der Leyen, Dear Commissioner McGrath,

We, the undersigned civil society organisations, academics, and other experts write to express our serious concern following the recent judgment of the United States Supreme Court *Trump v. Slaughter* and its implications for the European Commission's adequacy decision for the United States.

This judgment does not arise in isolation. It adds to long-standing concerns regarding whether the legal and institutional conditions underpinning Commission Implementing Decision (EU) 2023/1795 continue to exist. In particular, it calls into question assumptions on which the Commission expressly relied when concluding that the United States ensured a level of protection essentially equivalent to that guaranteed under European Union law.

The Commission's own adequacy decision recognised that independent supervisory authorities are indispensable to ensuring data protection in practice. It specifically relied on the independence of the Federal Trade Commission, including the safeguards protecting Commissioners from arbitrary removal. The recent judgment fundamentally alters that factual premise.

This matters far beyond the United States: the European Union has rightly presented adequacy as one of the strongest mechanisms for protecting people's rights when their personal data leaves the Union. That credibility depends on one simple principle. Adequacy decisions cannot become political endorsements that survive regardless of how legal and institutional circumstances evolve. They are legal findings that must be kept under continuous review.

Article 45 GDPR reflects exactly that understanding. It requires the Commission to monitor developments in third countries and to intervene where the conditions underpinning an adequacy decision are no longer met. This is not a discretionary political choice. It is a legal obligation.

The question before the Commission is therefore not whether transatlantic data flows are economically important; they are. Nor is it whether the European Union values cooperation with the United States; it does. The question is whether the factual findings on which the adequacy decision rests remain legally and institutionally justified.

That assessment cannot wait for years of litigation. Waiting until the Court of Justice is again asked to resolve questions that the Commission is already required to assess would repeat a cycle that has characterised EU-US data transfers for more than a decade. It would also undermine legal certainty for people, businesses and public authorities alike.

The implications extend well beyond the EU-US relationship. The adequacy framework is increasingly central to the Union's digital policy, international cooperation and global regulatory influence. Its legitimacy depends on the confidence that all adequacy decisions are reviewed according to the same objective legal standards, regardless of the country concerned or the geopolitical context.

At a time when the European Union faces increasing geopolitical pressure to weaken digital regulation in the name of competitiveness and transatlantic cooperation, the adequacy framework must remain anchored in law, not political expediency. Fundamental rights cannot become a bargaining chip in broader negotiations on trade, technology or security.

This review should also take account of the wider reality in which international data transfers now operate. Personal data transferred for commercial purposes does not exist in isolation. It may become accessible to public authorities through lawful requests, onward disclosures or the growing market for commercially available data. Recent revelations concerning the acquisition and use of commercially available data by law enforcement and immigration authorities demonstrate that the boundaries between commercial data ecosystems and state access are increasingly blurred. These realities must form part of any meaningful assessment of whether transferred data continues to benefit from an essentially equivalent level of protection.

We therefore call on the European Commission to:

- Immediately initiate a public reassessment of the implications of the recent US Supreme Court judgment, and other relevant factors, for Commission Implementing Decision (EU) 2023/1795.
- Publish its legal assessment of whether the factual findings underpinning the adequacy decision remain valid, including those relating to the independence and effectiveness of supervisory and oversight mechanisms.
- Consult the European Data Protection Board, the European Data Protection Supervisor, the Fundamental Rights Agency, independent academics and civil society organisations as part of that assessment.
- Reaffirm that adequacy is a living legal mechanism that requires continuous scrutiny, transparency and accountability, and that this principle applies equally to all existing and future adequacy decisions.
- If the Commission concludes that the conditions laid down in Article 45 GDPR are no longer fulfilled, take the measures required by the Regulation without delay.

The strength of the European Union's adequacy framework has never depended on the number of decisions it adopts. It depends on the willingness to review those decisions honestly when circumstances change. The Commission now has an opportunity to demonstrate that adequacy remains what the GDPR intended it to be: a living safeguard for fundamental rights, not a static political declaration. We urge you to seize that opportunity.

Yours sincerely,

AI Accountability Lab, Trinity College Dublin

Alternatif Bilisim

Asociația pentru Tehnologie și Internet (ApTI)

Ass.-Prof Dr. Soheil Human, Director of the Sustainable Computing Lab, Vienna University of Economics and Business

Associació Pangea

ASUFIN – Spanish Financial Users Association

Bits of Freedom

Centre for Democracy and Technology Europe

Cristiana Santos, School of Law Utrecht University

Data for Good

Data Privacy Brasil

Data Rights

Defend Democracy

Diaspora in Action for Human Rights and Democracy

Digihumanism – Centre for AI & Digital Humanism

Dr. Felix Bieker, FIZ Karlsruhe – Leibniz Institute for Information Infrastructure, Germany

Dr. Midas Nouwens, Associate Professor, Aarhus University

EDRi

Federación de Consumidores y Usuarios CECU

Glitch

Hermes Center Hacking for Human Rights

Institute for Digital Citizenship Foundation

IT-Pol Denmark

Lie Detectors

LobbyControl

Max Schrems

New School of the Anthropocene

noyb – European Center for Digital Rights

Open Markets Institute Europe

Open Rights Group

Panoptikon Foundation

People vs Big Tech

Politiscope

Raymond Amumpaire, Independent Digital Policy Analyst

Sophie Stalla-Bourdillon, Brussels Privacy Hub, LSTS, VUB

Stichting Data Bescherming Nederland

Transparency International EU