ICLE tl;dr

US-EU Data-Privacy Framework

October 2022

tl;dr

Background: On Oct. 7, President Joe Biden signed an executive order to implement the U.S.-EU data-privacy framework. The order had been awaited since March, when U.S. and EU officials reached an agreement in principle on a new framework, which EU officials insist must address concerns about surveillance practices by U.S. agencies. An earlier data-privacy framework was invalidated in 2020 by the Court of Justice of the European Union (CJEU) in its *Schrems II* judgment.

But: The European Commission will now consider whether to issue an "adequacy decision" for the U.S. This is urgent, because national data-protection authorities in the EU have been using a strained interpretation of the EU General Data Protection Regulation (GDPR) to prosecute various workarounds that companies have employed to transfer data between the U.S. and the EU. Like prior U.S.-EU arrangements, the order is likely to be challenged before the EU courts, but preliminary legal analysis suggests that this one has a greater chance of being upheld.

KEY TAKEAWAYS

WHY THE FRAMEWORK IS URGENT

In the *Schrems II* decision, the CJEU found that U.S. national-security law and the surveillance powers it grants to intelligence agencies do not provide adequate protection for the data of EU citizens. While the ruling denied the United States a national adequacy decision, the GDPR also permits firms that wish to transfer data to countries not deemed adequate to rely on "standard contractual clauses" (SCCs) to guarantee protection of citizen data. Some (including some in the European Parliament) have argued, however, that after *Schrems II*, no SCC can provide a lawful basis for data transfers to the United States.

Shortly after *Schrems II*, the Irish Data Protection Commission (IDPC) issued a preliminary draft decision against Meta that proposed to invalidate the company's SCCs. In July 2022, the IDPC circulated a draft decision that effectively would prohibit Meta from transferring personal data to the United States. Meta reported that such regulation might make it impossible for them to offer services like Facebook and Instagram in the EU.

Moreover, national data-protection authorities in Austria, Denmark, France, and Italy have concluded that Google Analytics' website monitoring services—which even the European Parliament itself uses—also violate the GDPR.

Given the trend among European authorities to regard the processing of personal data by U.S.-controlled entities to be illegal, even if the processing takes place entirely in Europe, without a new adequacy decision, it may soon become broadly impossible for U.S. businesses to offer tech services to EU citizens.

NEW FRAMEWORK SHOULD MEET EU LAW

The CJEU invalidated the prior adequacy decision on grounds that EU citizens did not have adequate redress under U.S. law and that U.S. law was not equivalent to "the minimum safeguards" of personal data protection under EU law. Early indications are that the European Commission believes the executive order addresses those concerns.

The new redress mechanism will create a civil liberties protection officer in the Office of the Director of National Intelligence, as well as a new Data Protection Review Court (DPRC). The DPRC is proposed as an independent review body that will make decisions that are binding on U.S. intelligence agencies.

The old framework had sparked concerns about the independence of the ombudsperson, and what was seen as insufficient safeguards about the external pressures that that individual could face, including the threat of removal. Under the new framework, the independence and binding powers of the DPRC are to be grounded in (as-yet unpublished) regulations issued by the attorney-general. This latter provision had been proposed by European legal academics Theodore Christakis, Kenneth Propp, and Peter Swire.

To address concerns about the necessity and proportionality of U.S. signals-intelligence activities, the executive order also defines the "legitimate objectives" in pursuit of which such activities can be conducted. These activities would, according to the order, be conducted with the goal of "achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside."

WHAT HAPPENS NEXT?

On the U.S. side, the attorney general will investigate whether to designate the EU (or its member states) as a "qualifying state for the purposes of the redress mechanism." This is important, because only citizens of "qualifying states" will be able to benefit from the new redress mechanism.

Given that the express purpose of the new U.S. framework is to enable U.S.-EU data flows, it is unlikely that the designation process ultimately will exclude the EU or its members. The U.S. government could, however, use this process to highlight that the safeguards covering personal data collection for intelligence purposes in some EU countries are not, in practice, more robust than those under the new U.S. framework.

On the EU side, the European Commission will prepare a draft adequacy decision and seek opinions from the European Data Protection Board, as well as from representatives of the member states. The European Parliament is also likely to express its nonbinding view. The Commission may make changes to the draft based on this consultation process and then adopt the decision.

For more on the importance of transatlantic data flows, see the ICLE-PPI issue brief *The Great Transatlantic Data Disruption* by Kristian Stout, Michael Mandel, and Mikołaj Barczentewicz. See also the ICLE explainer *Transatlantic Data Flows Are Crucial to Global Financial Services* by Kristian Stout and R.J. Lehmann.

CONTACT US

Mikołaj Barczentewicz
Senior Scholar
mbarczentewicz@laweconcenter.org

ICLE International Center for Law & Economics