
Update on the EU-US Data Privacy Framework

OCTOBER 10, 2022

On October 7, 2022, President Biden signed an [Executive Order](#) (“EO”) implementing the new trans-Atlantic EU-U.S. Data Privacy Framework (“EU-U.S. DPF”). The EU-U.S. DPF, previously [announced](#) by President Biden and the European Commission (“EC”) President Ursula von der Leyen in March of 2022, aims to foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union when, in 2020, it struck down the EC’s adequacy decision underlying the EU-U.S. Privacy Shield framework.

The new EU-U.S. DPF is comprised of two main parts. The first focuses on substantive safeguards for U.S. signals intelligence activities, requiring the necessary and proportionate collection of intelligence. The second sets forth a new redress mechanism to address complaints pertaining to data collection. This redress mechanism involves both the Civil Liberties Protection Officer in the Office of the Director of National Intelligence and a new independent Data Protection Review Court, established by the Attorney General.

The EO provides the EC with a [basis to adopt a new adequacy determination](#), restoring an important data transfer mechanism under European law. The adequacy determination process is expected to take around six months and will lead to a final adequacy decision being published in roughly March 2023.

Key Takeaways

Safeguards. The EO establishes substantive safeguards for signals intelligence activities including that such activities consider the privacy of all persons regardless of nationality or residency, be conducted only in pursuit of national security objectives, and be conducted only when necessary to advance validated intelligence priorities in a manner that is proportionate to such priorities. Legitimate objectives of such intelligence activities include protection against espionage, terrorism, foreign military capabilities,

cybersecurity threats and other such purposes. The President may authorize updates to the list of objectives in light of new national security imperatives.

New Redress Mechanism. The EO establishes a new redress mechanism with two levels of review to evaluate qualifying complaints concerning United States signals intelligence activities for any covered violation of United States law and, if necessary, provide appropriate remediation. Complaints coming from qualifying states will first go to Civil Liberties Protection Officer in the Office of the Director of National Intelligence (“CLPO”), who will conduct an initial investigation of the complaint and assessing potential remediation. This process aims to take into account relevant national security interests and applicable privacy protections.

As part of the second layer review, the EO establishes a [Data Protection Review Court](#) (“DPRC”). The goal of the DPRC is to provide independent and binding review of the CLPO’s decisions, upon an application from the complainant or an element of the Intelligence Community. The DPRC will consist of non-government officials acting as judges. In other words, during their term of appointment on the DPRC, such judges shall not have any official duties or employment within the United States Government other than their official duties and employment as judges on the DPRC. The EO also provides for the DPRC to select a special independent advocate in each case who will advocate for the complainant’s interest in the matter and ensure that the DPRC is well-informed of the issues and the law with regard to the matter. After a DPRC review is complete the CLPO shall be informed of the decision, and the complainant will be informed through the appropriate public authority in a qualifying state. The DPRC’s decisions shall have binding effect on the intelligence community and the Attorney General shall not interfere with a review by a DPRC. The DPRC may also provide a classified report on information indicating a violation of any authority subject to the oversight of the U.S. Foreign Intelligence Surveillance Court (“FISC”) and such information will be raised to the FISC.

Updates on Policies. The EO calls for updated policies and procedures to reflect its new safeguards. The head of each element of the Intelligence Community shall within one year of the date of the EO, in consultation with the Attorney General, the CLPO, and the Privacy and Civil Liberties Oversight Board (“PCLOB”), update the policies and procedures as necessary to implement the privacy and civil liberties safeguards in the EO. The PCLOB will be charged with the task of reviewing the policies. It has issued a [statement](#) indicating that it plans to accept the advice and oversight roles envisioned in the EO.

Immediate impact for companies. [European trade associations](#) have asked European data protection authorities to refrain from issuing fines or prohibiting transfers until the new EC adequacy decision is formally adopted, but there are no guarantees in this regard. It is widely expected that there will be legal challenges against the new adequacy decision, but only the Court of Justice of

the European Union has the power to declare such EC decision invalid.

In the meantime, companies should keep an eye out for updated guidance and procedures from the U.S. government relating to implications for current data transfers and how to participate in the DPF.

It is worth noting that the EO does not appear to be limited to personal data transferred under the Privacy Shield framework, so the EO will also have positive effects on transfers of personal data from the EU based on Standard Contractual Clauses or Binding Corporate Rules.

The United Kingdom will not be covered by any EC adequacy decision, but the UK and the U.S. have announced on October 7, 2022, that they are also [moving towards a data adequacy agreement to benefit businesses and boost digital trade](#).

Authors



Kirk J. Nahra

PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



**Dr. Martin
Braun**

PARTNER

✉ martin.braun@wilmerhale.com

☎ +49 69 27 10 78 207



Tamar Y. Pinto

SENIOR ASSOCIATE

✉ tamar.pinto@wilmerhale.com

☎ +1 617 526 6151