

October 7, 2022

Biden Issues Executive Order to Implement U.S. Commitments Under the EU-U.S. Data Privacy Framework

On October 7, 2022, President Biden issued the “Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities” (the “EO”),¹ directing steps the U.S. will take to implement commitments agreed to under the European Union-U.S. Data Privacy Framework (“EU-U.S. DPF”) in March 2022.² The EO details key steps to strengthen privacy and civil liberties safeguards for U.S. signals intelligence activities and creates mechanisms for individuals to seek redress for the collection of personal information through intelligence activities in violation of applicable U.S. law.

The EO sets out measures that are intended to address the concerns raised by the Court of Justice of the EU when it struck down the EU-U.S. Privacy Shield framework as a valid means under which to transfer personal information of EU data subjects to the U.S.. The EO will likely bring the EU and U.S. closer to reestablishing a basis for transatlantic data flows that would be an alternative to the current regime, under which Companies must enter into Standard Contractual Clauses or Binding Corporate Rules to lawfully facilitate transfers of personal information from EU to the U.S.

Key Takeaways from the EO:

- **New privacy and civil liberties safeguards:** The EO imposes an array of privacy and civil liberties safeguards on U.S. signals intelligence activities, including:
 - A requirement that U.S. signals intelligence activities be conducted only in pursuit of defined national security objectives and be restricted to settings where such activities are necessary to advance a validated intelligence priority and are implemented in a manner proportionate to that priority. Under the EO, signals intelligence activities must take account of the privacy and civil liberties of all persons, regardless of nationality or country of residence. These measures thus mark a key expansion from prior protections, which focused only on U.S. persons.
 - New data handling requirements for the treatment of personal information collected through signals intelligence activities.

¹ The White House, *Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities* (Oct. 7, 2022), <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/>;

² The White House, *Fact Sheet: United States and European Commission Announce Trans-Atlantic Data Privacy Framework* (Mar. 25, 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/>;

- Affirmative obligations for legal, oversight and compliance officials to take appropriate action to remediate incidents of non-compliance, and for the intelligence community to implement updated policies and procedures incorporating these changes.
- **Creation of an adjudication process with authority to issue binding decisions:** The EO also creates a novel mechanism within the Executive Branch to adjudicate claims brought by individuals that their personal information was collected in violation of applicable U.S. law, including the new heightened protections outlined in the EO.
 - Individuals from qualifying states and regional economic integration organizations designated by the Attorney General may submit complaints for review by the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (“CLPO”). After investigation of the claims to determine if a violation has occurred, the EO grants the CLPO authority to issue binding decisions on the intelligence community. Importantly, the EO also adds protections to ensure the CLPO’s investigations and determinations remain independent.
 - The EO directs the Attorney General to establish a Data Protection Review Court (“DPRC”) to review the decisions issued by the CLPO. Review by the DPRC is triggered only upon an application from the individual bringing the complaint, or an entity within the intelligence community. Judges of the DPRC are to be hired from outside the U.S. government and must have relevant experience in data privacy and national security. The DPRC’s decisions as to whether a violation of U.S. law has occurred and how to remediate any violation will also be binding. The EO also provides for a special advocate to be appointed by the DPRC to advocate regarding the complainant’s interest and to inform the DPRC on issues of both law and fact. The constitutionality of such a reform has been long-debated in the FISA context.³
- **Provides for oversight of compliance by intelligence community.** Finally, the EO directs the Privacy and Civil Liberties Oversight Board (“PCLOB”) to review the policies and procedures of the intelligence community to ensure compliance with the EO—as well as to ensure, on an annual basis, that the intelligence community has complied fully with the determinations made by the CLPO and DPRC.

The steps provided for by the EO appear designed to set forth a data protection regime sufficient for the European Commission to adopt a new adequacy determination regarding data transfers to the U.S. If they are found to provide adequate protections, the steps in the EO would likely enable the creation of a long-awaited replacement for the EU-U.S. Privacy Shield framework that was struck down in July 2020, providing a less burdensome and more cost-effective mechanism for entities to conduct transatlantic data transfers.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Ross M. Gotler
+1-212-373-2979
rgotler@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associate Cole A. Rabinowitz contributed to this Client Memorandum.

³ See Marty Lederman and Steve Vladeck, LAWFARE, *The Constitutionality of FISA “Special Advocate”* (Nov. 4, 2013), <https://www.justsecurity.org/2873/fisa-special-advocate-constitution/>;