Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

President Biden Signs Long-Awaited Data Transfer Executive Order

October 19, 2022

Key Points

- President Biden has signed the long-awaited executive order implementing U.S. commitments to the new successor agreement to the Privacy Shield, the EU-U.S. Data Privacy Framework—a historic step in respect of trans-Atlantic data transfers.
- The executive order creates a new two-tier redress mechanism for individuals in the EU (namely lodging complaints before a Civil Liberties Protection Officer and further having the possibility of appealing the decision of such an officer before a newly created Data Protection Review Court) and also establishes a number of additional safeguards which constitute a substantive limitation on the U.S. intelligence communities access to and handling of data.
- The European Commission will now commence its approval process, and EU officials continue to project that a new trans-Atlantic data flow agreement could be in place as early as March 2023.

Background and Implications

On March 25, 2022, President Biden and European Commission President von der Leyen announced that they had reached an agreement in principle on a new European Union (EU)-U.S. Data Privacy Framework (EU-U.S. DPF) (see our previous alert here). Subsequently, on October 7, 2022, President Biden signed the long-anticipated executive order (EO) on Enhancing Safeguards for United States Signals Intelligence Activities, outlining key directives to implement the U.S.' commitments under the EU-U.S. DPF.

The EU-U.S. DPF seeks to foster trans-Atlantic data flows and further aims to address the concerns raised by the Court of Justice of the EU when it struck down the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield framework in 2020. The European Commission will now (i) prepare a draft adequacy decision and (ii) commence its adoption process, which is expected to take approximately six months, with the new agreement potentially being ready as soon as March 2023, although this timeline could slip given the pace of the process thus far.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Ed Pagano
Partner
epagano@akingump.com
Washington, D.C.
+1 202.887.4255

Jenny Arlington
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

Galen A. Roehl
Senior Policy Advisor
groehl@akingump.com
Washington, D.C.
+1 202.887.4224

Taylor Daly
Policy Advisor
tdaly@akingump.com
Washington, D.C.
+1 202.416.5541

Sahar Abas
Associate
sahar.abas@akingump.com
Dubai
+971 4.317.3052

As noted by the European Commission's response to the EO, a number of other EU institutions will be involved in reviewing the EU-U.S. DPF. The European Commission will obtain an opinion from the European Data Protection Board (EDPB) and seek the approval of a committee comprised of the representatives of the EU Member States; the European Parliament also retains the right to oversee adequacy decisions. It is only once the review by the relevant EU institutions has been completed that the European Commission can adopt the final adequacy decision in respect of the U.S. and, thereafter, allow data to flow freely between the EU and U.S. companies certified by the U.S. Department of Commerce under the EU-U.S. DPF.

While significant, the EO does not replace existing U.S. surveillance laws and instead applies alongside such laws (importantly applying to both U.S. and non-U.S. persons in respect of the data collection activities of U.S. surveillance agencies); the EO serves to add additional protections for individuals in respect of the activities of the U.S. intelligence community and is an important development following the two-year negotiation between the EU and the U.S. on trans-Atlantic data transfers. Organizations transferring personal data, which is very broadly defined under the EU's General Data Protection Regulation (GDPR) such that most organizations will be caught by this, to the U.S. should closely monitor the European Commission's approval proposal, the issuance of any adequacy decision and the actions undertaken by the U.S. intelligence community in response to the directions under the EO. We set out below a summary of the two key features of the EO: (i) the redress mechanism and (ii) establishment of significant requirements in respect of intelligence activities.

Redress Mechanism

The EO establishes a novel two-tier redress mechanism, namely:

(i) Lodging a Complaint with the Civil Liberties Protection Officer (CLPO): By December 6, 2022, the Director of National Intelligence must establish a process for the submission of qualifying complaints, in addition to a process authorizing the Office of the Director of National Intelligence's (ODNI) CLPO to investigate, review and order appropriate remediation for complaints. Subject to (ii) below, the EO expressly notes that each element of the U.S. intelligence community must comply with any determinations made by the CLPO.

(ii) Appealing Decisions of the CLPO to a Newly Established Data Protection Review Court (Court): The EO authorizes and directs the Attorney General to establish a process to independently review determinations made by the CLPO via the newly-created Court. By December 6, 2022, the Attorney General must issue regulations establishing the Court, which will be comprised of three appointed judges who are legal practitioners in the fields of data privacy and national security (and not within the U.S. government). The Court will be tasked with impartially reviewing the determinations made by the CLPO with respect to whether a covered violation occurred and determining the appropriate remediation; importantly, decisions of the Court will be binding. Pursuant to the EO, the Court will also select a special advocate to advocate on behalf of the complainant in each case.

The EO prohibits the Attorney General from interfering with the Court's review or removing any judges, save for instances of misconduct. The regulations promulgated by the Attorney General will outline the required procedures for transmitting determinations. This is a significant development from the mechanisms that existed at

the time of the Privacy Shield whereby individuals' primary form of redress was via the Ombudsperson who did not have the impartiality or investigatory and decision-making powers now afforded to the Court.

The EO further directs the Attorney General to designate a country as a "qualifying state" for purposes of the redress mechanism, granting discretion in determining the effective date of the designation. Under the EO, a "covered violation," must, among other criteria, arise from activities related to data transferred to the U.S. from a qualifying state, and complaints must be transmitted by the appropriate public authority in a qualifying state to the CLPO. The EO stipulates that a state designation can be revoked if: (1) the country in question does not provide sufficient safeguards for the U.S.'s personal information, (2) the country does not permit the transfer of personal information for commercial purposes to the U.S. or (3) the designation is not in the national interests of the U.S.

The Commerce Department is tasked with maintaining a record of complaints. In addition, the Privacy and Civil Liberties Oversight Board (PCLOB) is encouraged to conduct an annual review of the processing of complaints, reviewing timeliness, efficiency and compliance with the EO's requirements.

Significant Requirements for Intelligence Activities

In addition to the novel redress mechanisms now afforded to individuals, the EO outlines a number of principles for U.S. intelligence activities to adhere to, including that such activities must: (1) be authorized by statute or by EO, proclamation or other Presidential directive and in line with existing laws and Presidential directives; (2) be subject to appropriate safeguards, including that such activities be conducted only following a determination that they are necessary to advance a legitimate intelligence priority, and only to the extent that is proportionate to the priority; and (3) be subjected to "rigorous" oversight.

In an effort to address the concerns raised by the Court of Justice of the EU, the EO establishes a number of additional safeguards and obligations. For example, U.S. intelligence agencies are required to update their policies and procedures in order to implement the privacy and civil liberty safeguards in the EO, must also have in place senior-level legal, oversight and compliance officials tasked with conducting periodic oversight of signals intelligence activities and must further adhere to limitations on the retention of personal data.

In carrying out its existing responsibility of presenting the National Intelligence Priorities Framework (NIPF) to the President on a regular basis, the order stipulates that ODNI must first obtain an assessment from the CPLO of whether each of the priorities advance a legitimate objective and considers privacy and civil liberties of all persons. The EO points to a total of 12 legitimate objectives, including assessing the capabilities or activities of a foreign government, a foreign military and certain foreign organizations, in addition to protecting against foreign military capabilities, terrorism, espionage, the proliferation of weapons of mass destruction and cybersecurity threats. While the EO permits the bulk collection of signals intelligence, the EO narrows the legitimate objectives for which such collection must relate, further requiring that targeted collection be prioritized wherever possible.

Significantly, the EO expressly confirms that certain objectives are not legitimate and thereby prohibited, including intelligence collection activities related to suppressing

criticism, free expression, legitimate privacy interests or a right to legal counsel, in addition to those that discriminate based on certain factors such as ethnicity, race or gender. The collection of private commercial information or trade secrets to afford a competitive advantage to U.S. companies and business sectors are further expressly not legitimate objectives and subsequently prohibited.

With regard to timeline, the EO directs the head of each element of the intelligence community to implement the privacy and civil liberties safeguards in the EO and release the procedures publicly, to the extent possible, by October 7, 2023. In "significant" incidents of non-compliance, the EO requires each element of the intelligence community to report incidents promptly to the head of the element, in addition to the head of the applicable agency and the Director of National Intelligence. The EO's definition of "elements" of the intelligence community is in line with Executive Order 12333, which outlines a total of 15 offices, in addition to any other office determined by the President to be an element.

Conclusion

This is a major welcomed development, although it remains to be seen if it will withstand the scrutiny of activists like Max Schrems, who already said he will likely challenge it again. Akin Gump continues to monitor implementation of the EO, in addition to its review by EU institutions, and will continue to keep clients apprised of key developments.

akingump.com