PUBLICATION

New Executive Order Aims to Restore U.S.-EU Data Privacy Agreement

Authors: Alisa L. Chestler, Aldo M. Leiva
October 10, 2022

On October 7, President Biden signed an Executive Order directing the federal government to implement U.S. commitments under the European Union-U.S. Data Privacy Framework (EU-U.S. DPF). The new Executive Order enhances safeguards and privacy policies governing U.S. signals intelligence (SIGINT) activities to restore the trust relationship between the U.S. and the EU required for data transfer under EU law.

Under the EU's General Data Protection Regulation (GDPR), the European Commission (EC) has the power to determine whether the privacy laws of a nation outside the EU are sufficient to protect the privacy rights of European citizens. If the EC determines a nation's laws or practices to be inadequate, it can bar the transfer of data from the EU to any organization in that country. In making adequacy decisions, the EC considers rule of law, human rights, data protection rules, and access by public authorities to personal data, amongst others.

In July 2020, the Court of Justice of the European Union (CJEU) issued a judgment declaring as "invalid" the European Commission's Decision (EU) 2016/1250 of July 12, 2016, on the adequacy of the protection provided by the EU-U.S. Privacy Shield. As a result of that decision, the Privacy Shield Framework is no longer a valid mechanism to transfer personal data from the EU to the U.S. The aim of this Executive Order is to provide the EC with justification to revisit its adequacy decision, restore the trust relationship between the U.S. and the EU, and re-establish a clearly defined data transfer mechanism for U.S. businesses consistent with the EU laws.

Background

The Executive Order is the latest step in efforts of the U.S. to implement the EU/U.S. DPF that was announced in March 2022, to address the uncertainty surrounding transatlantic data flows following the annulment of the Privacy Shield in 2020 by the EU Court of Justice in its *Schrems II* judgment.

The *Schrems II* ruling held that the Privacy Shield did not offer adequate protection for EU-U.S. data flows because U.S. government surveillance practices were too intrusive. While the *Schrems II* ruling upheld the legality of Standard Contractual Clauses (SCCs) to export data out of Europe, it also required suspension of data transfers to any country where EU standards are not met. *Schrems II* judgment was issued in the aftermath of the well-publicized revelations of National Security Agency (NSA) bulk data collection programs by former contractor Edward Snowden in 2013. In the leaks of classified documents, Snowden revealed numerous global surveillance programs operated by the NSA and other allied intelligence agencies.

The Privacy Shield replaced the Safe Harbor Framework in 2016, which had been declared invalid by the CJEU in 2015 in its *Schrems I* decision.

Executive Order

The new Executive Order directs several significant changes to the way in which the U.S. Intelligence Community (IC) operates to ensure adequate protections of the privacy and civil liberties of both U.S. and European citizens. These include:

- **Enhancing Safeguards for SIGINT Collection:** The Executive Order directs that SIGINT collection activities shall only be conducted to advance a validated intelligence priority, with due consideration for proportionality of data collected, and weighed against the privacy and civil liberties of "all persons, regardless of their nationality or wherever they might reside." This marks a significant departure from current SIGINT policies, such as Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, which only extend these protections to U.S. persons and the citizens of certain allies.

- **Narrowing the Objectives of SIGINT Collection:** Under the Executive Order, SIGINT activities may only be undertaken to understand and assess the capabilities and intentions of foreign nations and organizations and to protect against transnational and cybersecurity threats. Specifically prohibited objectives include suppressing civil liberties, such as free expression, and targeting foreign companies for the purpose of economic espionage.

- **Limiting Bulk Collection:** The Order prioritizes collection against validated individuals. One of the primary contentions of the EU in invalidating Privacy Shield was the NSA's bulk collection of data. Bulk collection will now require authorization by the head of an element of the IC and may only be conducted to protect against terrorism, espionage, weapons of mass destruction, cybersecurity threats, and transnational criminal threats.

- **Handling of Personal Information:** Each element of the IC will be required to establish and apply agency-specific policies and procedures to minimize the retention and dissemination of all personal information. Notably, IC elements must apply the same rules for the retention of the personal information of foreign nationals as it has historically applied to retaining U.S. persons' information.

- **Updating Policies and Procedures:** In consultation with the Privacy and Civil Liberties Oversight Board (PCLOB), IC elements have one year to update their policies and procedures related to SIGINT activities to implement the privacy and civil liberties safeguards required by the Executive Order.

- **Establishing a Redress Mechanism:** The Executive Order creates a multi-layer mechanism through which individuals from qualifying states and organizations can obtain an independent binding review and redress for violations of their civil liberties by U.S. SIGINT activities. This includes the establishment of a Civil Liberties Protection Officer (CLPO), charged with conducting initial investigations of complaints to determine validity and redress, and a Data Protection Review Court, comprised of judges from outside the U.S. Government, imbued with the authority of the Attorney General to review decisions by the CLPO.

Implications for U.S. Businesses

In the digital era, EU data protection laws apply to U.S.-based companies with significant consequences. The EU law generally prohibits the transfer of personal data from the EU to the U.S. unless the transfer is made in accordance with one of a very few of authorized data transfer mechanisms or otherwise falls within one of its even fewer exceptions. This transfer restriction significantly impacts U.S. multinational companies' everyday business activities. Privacy Shield (along with its predecessor, the Safe Harbor Framework) was fairly popular among U.S. companies because of its flexibility and low cost.

Due to the *Schrems I* and *II* decisions, thousands of U.S.-based companies that previously relied on the Privacy Shield program to transfer EU data to the U.S. were left in the limbo. Many of them were forced to invest significant resources in other data transfer mechanism such as the SCCs and the Binding Corporate Rules, which are more expensive and cumbersome to implement. Some of those companies made the

business decisions to stop all data transfers between the EU and the U.S. entirely. This Executive Order is an important step towards a more reliable and affordable data transfer mechanism between the EU and the U.S.

What's Next?

The EC will now conduct its adequacy assessment by reviewing this Executive Order and the steps taken by the IC in making its revised adequacy decision. Stakeholders and experts have anticipated that this process might take about six months. If successful, this order will usher in a new transatlantic data sharing agreement affecting thousands of businesses across the country. New policies and procedures likely will follow, along with new opportunities for growing business in the European market. Following an adequacy determination, companies will be able to self-certify to the EU-U.S. DPF's commercial principles.

How Does This Executive Order Affect the SCC and the Transfer Impact Assessment?

Following the *Schrems II* decision in 2020, the SCC mechanism has been the only realistic choice for many U.S.-based companies. As provided by the new SCCs issued by the EC in June 2021, data controllers or processors are required to conduct a Transfer Impact Assessment prior to transferring EU data to the U.S. Among other things, a Transfer Impact Assessment establishes whether the laws of the third country in question would allow government agencies of that third country to access the personal data.

Until an adequacy decision is made for the EU-U.S. DPF, companies should continue to use existing mechanism deemed by the EC to be sufficient, including the SCCs, and follow the European Data Protection Board's recommendations on supplement transfer tools to ensure compliance with the E.U. level of protection (reference here). Since this Executive Order has taken effect, companies currently conducting Transfer Impact Assessments should reference and discuss this new Executive Order when analyzing the impact of U.S. surveillance laws. Due to the complexity of this exercise, companies relying on SCCs for their transfers should engage competent legal counsel with an understating of this new Executive Order to assist them with conducting Transfer Impact Assessments and drafting annexes of the SCCs.

Once the EU-U.S. DPF is available for companies to self-certify, the costs and uncertainty associated with conducting Transfer Impact Assessments and supplementary measures might be eliminated. Companies interested in how the EU-U.S. DPF will impact existing privacy policies and how the self-certification process will be implemented should stay tuned for further updates from Baker Donelson's Data Protection, Privacy, and Cybersecurity Group.

If you have any questions about the impact of this Executive Order and what your business should do in the interim to transfer data from EU to the U.S., please contact Alisa L. Chestler.