CARTER/LEDYARD

our resources

The Biden Administration's Executive Order on EU-U.S. Data Transfer Framework: What's Next?

October 26, 2022

Earlier this month, President Biden took a key step towards removing barriers to the cross-Atlantic transfer of personal data from Europe to the United States. On October 7, 2022, he signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities ("Executive Order"), which reinforces the U.S. commitments announced last March by the Biden Administration and European Commission President Ursula von der Leyen to re-establish a legal regime governing data transfers from the EU to the U.S.

This marks the latest step toward implementing the EU-U.S. Data Privacy Framework ("DPF"), a replacement for the now defunct EU-U.S. Privacy Shield program that the Court of Justice of the European Union ("CJEU") invalidated in July 2020 with its *Schrems II* decision.[1] If approved, the DPF promises to restore a legal basis for the cross-border transfer of personal information from the EU to the U.S. by addressing concerns flagged by the CJEU regarding the expansive data collection activities of U.S. intelligence agencies and the lack of judicial remedies under U.S. law for EU data subjects whose data is collected by those agencies.

Key Aspects of the Executive Order

The Executive Order focuses on creating and enhancing safeguards for U.S. national security agencies' use of and access to EU and U.S. personal data. It also creates an independent and binding dual-layer mechanism enabling individuals in qualifying states to seek review and redress of claims that their personal data was collected or handled by U.S. intelligence agencies in a manner that violated U.S. law. In particular, the Executive Order:

- *Adds safeguards for U.S. signals intelligence activities*: The Executive Order mandates that U.S. signals intelligence activities shall be conducted only in pursuit of defined national security objectives, taking into account the privacy and civil liberties of all persons (regardless of nationality or country of residence), and only to the extent necessary and proportionate to advance a validated intelligence priority. The Executive Order also specifies certain "legitimate objectives" and "prohibited objectives" for U.S. signals intelligence activities.

- *Mandates handling requirements for personal information*: The Executive Order mandates certain minimization, dissemination, retention, data quality, and documentation requirements for the safe handling of personal data by intelligence agencies, including the implementation of remediation activities in the event of non-compliance.

- *Creates a dual-layer mechanism for the review and redress of claims*: The Executive Order creates a two-tiered mechanism for individuals from certain states and regional economic integration organizations to have independent review and binding redress of claims regarding the collection or handling of their personal data in violation of applicable U.S. laws. Under the first layer, the Civil Liberties Protection Officer in the Office of the Director of National Intelligence ("CLPO") will conduct an initial investigation of qualifying complaints received to determine whether the Executive Order's enhanced safeguards or other appliable U.S. laws were

violated and, if so, to determine the appropriate remediation. As a second layer of review, the Executive Order directs the U.S. Attorney General to establish a Data Protection Review Court ("DPRC") to provide independent and binding review of the CLPO's decisions. The DPRC's judges will be appointed from outside the U.S. government and have relevant experience in the fields of data privacy and national security.

- *Requires the update and continuous review of U.S. Intelligence Community policies and procedures*: The Executive Order requires U.S. intelligence agencies to update their policies and procedures to reflect the privacy and civil liberties safeguards contained in the Executive Order. It also calls on the Privacy and Civil Liberties Oversight Board ("PCLOB") to review these policies and procedures to ensure consistency with the Executive Order, and to conduct an annual review of the Executive Order's redress process, including whether the Intelligence Community has fully complied with determinations made by the CLPO and the DPRC.

Next Steps

The next steps will be for the European Commission to review the DPF, issue a draft adequacy decision, and launch its adoption procedure. This is a multi-step process expected to take up to six months. As part of the process, the European Commission will prepare a draft adequacy decision, and the European Data Protection Board ("EDPB") will then submit the draft decision for review by a committee composed of representatives of the EU member states. Once this review is complete, the European Commission can proceed to adopt a final adequacy decision.

If it is determined that the U.S. commitments under the DPF meet the EU's General Data Protection Regulation's ("GDPR") "adequacy" standard, businesses certified under the DPF will be able to transfer personal data from the EU to the United States without having to rely on alternative data transfer mechanisms, such as Standard Contractual Clauses ("SCCs") and Binding Corporate Rules ("BCRs").

If adopted, the DPF is likely to face legal challenges before the EU courts. Indeed, a number of privacy advocacy groups have already issued statements opining that the Executive Order does not go far enough to allay the concerns raised by the CJEU in its *Schrems II* decision. For example, NOYB—the privacy non-profit led by Max Schrems—issued a first reaction to the Executive Order, concluding that it is unlikely to satisfy EU law.

Should the DPF be adopted and not struck down, U.S. companies would be able to join the framework by committing to comply with a detailed set of privacy obligations, under a program to be administered by the U.S. Department of Commerce. While these obligations have not yet been detailed, it is expected that they will entail certain core principles, such as minimizing data being transferred, limiting the purposes for which data is transferred, and affording certain rights to data subjects.

In the Meantime

Until a final adequacy decision is adopted, businesses engaged in cross-border transfers of personal data from the EU should continue to follow the EDPB's recommendations on measures that supplement transfer tools. In particular, businesses may still rely on other valid data transfer mechanisms, including SCCs and BCRs. SCCs, which are the most common mechanism for EU-U.S. data transfers, allow businesses to transfer data if they incorporate certain model clauses into their commercial contracts. In June of last year, the European Commission formally adopted new SCCs for international personal data transfers from the EU. As of September 27, 2021, all new data transfer agreements are required to incorporate the new SCCs. **Businesses have until December 27 of this year to migrate existing SCC arrangements to the new SCCs**.

Conclusion

Given the time required for implementation of the Data Privacy Framework and the near certainty of further legal challenges, companies are encouraged to stay current on alternative compliant data transfer mechanisms (and any additional transfer obligations required by the EDPB's

guidance). If you have questions about how to transfer data from the EU in compliance with the GDPR, it is encouraged that you speak to your data privacy or cybersecurity law attorney at Carter Ledyard.

* * *

---

[1] For more information about the *Schrems II* decision and its effects on the transfer of personal data between the EU and the U.S., see our April 22, 2021 article *EU-US Transfers of Personal Data in the Wake of the* Schrems II *Ruling*.

---

related professionals

Sarah H. Ganley / Associate
D 212-238-8834
ganley@clm.com

Jodutt Marwan Basrawi / Associate
D (212) 238-8767
basrawi@clm.com