THE NEW EUROPEAN UNION-U.S. DATA PRIVACY FRAMEWORK: WILL IT BE "BRAVE NEW WORLD" OR "GROUNDHOG DAY"?

Mathea K. E. Bulander

This past March, the EU and the U.S. reached an agreement in principle regarding a new EU-U.S. Trans-Atlantic Data Privacy Framework ("TADPF"). On Friday, October 7, 2022, more than six months after reaching the agreement, President Biden issued the Executive Order, viewed as necessary, to finalize that agreement. There is hope that this greatly anticipated order will secure U.S. companies' path toward "restor[ing] trust and stability to transatlantic data flows and reflects the strength of the enduring EU-U.S. relationship based on our shared values."[1] Yet, even though the Executive Order addresses the key issues raised by *Schrems II*[2], the death knell for the prior Privacy Shield, questions remain regarding the speed at which the EU Commission may approve the Order, or not, and whether agreement based upon an executive order will provide any real and lasting stability regarding EU data transfers.

Last spring, when it announced the TADPF, the European Commission outlined five key principles of the agreement:

- Data will be able to flow freely and safely between the EU and participating U.S. companies;
- A new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security; U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards;
- A new two-tier redress system to investigate and resolve complaints of Europeans on the access of data by U.S. intelligence authorities, which includes a Data Protection Review Court;
- Strong obligations for companies processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce; and
- Specific monitoring and review mechanisms.[3]

---

[1] White House Press release, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.
[2] Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd., (Maximillian Schrems), [2021] W.L.R. 751, ECLI:EU:C:2020:559 (Jul. 16, 2020).
[3] *See* https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100.

The Executive Order addresses the requirements for binding safeguards and a multi-tier redress system in significant detail. Section 2 of the Order outlines extensive requirements for permissible signals intelligence, advancing the principle that "signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized," outlining provisions for bulk collection of signals intelligence, and providing extensive examples of legitimate objectives for signals intelligence collection actives, as well as prohibited objectives. Section 3 establishes the two-tier redress system, creating an initial investigation by the Civil Liberties Protection Officer of the Office of Director of National Intelligence, the establishment of the new highly-anticipated Data Protection Review Court (which was also established on October 7, 2022), by a Rule issued by Attorney General Merrick Garland pursuant to 28 U.S.C. §§ 511 and 512)[4], and annual review by the Privacy and Civil Liberties Oversight Board, complete with myriad cross-check protocols. Thus, it appears there is a good chance that the EU may agree that points two and three of the TADPF agreement have been satisfied.

Less clear is whether the EU may require any updates to data processing obligations not addressed by the Executive Order to satisfy the TADPF agreement. TADPF compliance will certainly include self-certification by the U.S. Department of Commerce ("U.S. DOC"), as was required under the Privacy Shield. Companies should expect that many of the general processing requirements established by Privacy Shield will be reaffirmed under the oversight of the U.S. DOC as a part of the "strong obligations for companies processing data." But there is little in the Executive Order to help forecast how the EU and U.S. will achieve a meeting of the minds regarding any particular processing requirements.

As a result, companies working to manage Trans-Atlantic business with the EU member nations continue to face significant uncertainty, at least in the short term. Moreover, even assuming that the U.S. proposal is accepted without amendment, organizations should expect that it will take many months before the EU Commission can draft a written proposal for the European Data Protection Board, which must then review and issue an opinion regarding the proposal that will subsequently be evaluated by a committee of EU member states, and then finally, if the committee approves, the European Commission formally issues an adequacy decision for the new framework, finding that it provides protections for EU data that are essentially equivalent to those under the EU General Data Protection Regulation ("GDPR").

The uncertainty does not end with an adequacy determination, however. An agreement and adequacy determination secured by an executive order may last only as long as the current administration (2015 Paris Agreement anyone?). As is always the case with an executive order, no checks and balances would prevent another administration from circuitously changing the U.S. practices established to secure the TADPF approval. In the short term, businesses are wise to manage this risk by preparing multiple options for compliance with the GDPR and EU adjacent rules.

---

[4] *See* https://www.justice.gov/opcl/page/file/1541321/download.

Flexibility is particularly prudent in light of the fact that the guidance for standard contractual clauses ("SCCs") was changed in 2021, and all current contracts must meet the new compliance guidelines by December 27, 2022. Even if the contracts are updated, however, companies may face yet another need to pivot. In July 2022, Ireland's privacy regulator decided to block Facebook's use of SCCs. This decision has not yet been approved by other authorities in Europe, but its prospect further attenuates U.S. certainty regarding the stability of EU and U.S. commerce. One goal of the TADPF is to further secure not only an agreement between the EU and the U.S. regarding the U.S. regulatory scheme, but also to resolve the outstanding questions regarding SCCs and binding corporate rules. Such increased stability would be welcome news for many.

In the interim, there is an opportunity for organizations and their counsel to evaluate the requirements and begin to assess the multiple paths to ensure business continuity and to prepare themselves to change course as new requirements are clarified.

For assistance with or additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.