Published on *The National Law Review* https://natlawreview.com

The U.S. and EU Announce an "Agreement in Principle" to Replace the EU-U.S. Privacy Shield Framework: What Employers Need to Know

Article By:

Simon J. McMenemy

Grant D. Petersen

Salvatore A. Anania

On March 25, 2022, the European Union (EU) announced that the United States and the EU had reached an agreement in principle to replace the EU-U.S Privacy Shield framework, which the European Court of Justice (CJEU) struck down in its July 2020 *Schrems II* decision. Since the *Schrems II* decision, U.S. and EU negotiators have been hammering out a workable data transfer mechanism to permit the transfer of EU data to the United States.

What does the agreement provide?

The White House and European Commission each issued fact sheets that outline some of the details of the new agreement. The new data transfer framework will be called the "Trans-Atlantic Data Privacy Framework" (TADPF) and will address the concerns raised by the CJEU in the *Schrems II* decision regarding the expansive data collection activities of U.S. intelligence agencies and the lack of judicial remedies under U.S. laws for EU data subjects whose data is collected by these agencies. Specifically, the TADPF will ensure that:

- Binding safeguards will be in place to limit access to data by U.S. intelligence agencies to what is necessary and proportionate to protect legitimate national security objectives and will not disproportionately impact the protection of individual privacy and civil liberties;
- EU individuals will be able to seek redress for any improper collection of data by U.S. intelligence agencies from a new multi-layer redress mechanism that includes an independent Data Protection Review Court that will consist of individuals chosen from outside the U.S. government who will have full authority to adjudicate claims and direct remedial measures as needed; and
- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy

and civil liberties standards.

Companies and organizations that implement the TADPF will be required to comply with many of the Privacy Shield principles, including the requirement to self-certify their compliance through the U.S. Department of Commerce. Additionally, like under the Privacy Shield, EU individuals will continue to have access to multiple avenues of recourse to resolve complaints against participating TADPF organizations, including through alternative dispute resolution and binding arbitration.

What are the next steps for the new framework?

The U.S. government and the European Commission will translate this agreement into legal documents that will need to be adopted on both sides to implement the TADPF. The United States will document its commitments in an executive order that will form the basis of the European Commission's assessment in its future adequacy decision.

Thereafter, the European Commission must follow a multi-step process for issuing the adequacy decision for the new framework. First, the EU Commission must draft a written proposal for the adequacy decision. Second, the European Data Protection Board (EDPB) must review and issue an opinion regarding the proposal. Third, representatives of the EU countries must approve the proposal. Fourth and finally, the European Commission must formally issue an adequacy decision finding that the new framework provides protections for EU data that are essentially equivalent to those provided under EU law, i.e., the EU General Data Protection Regulation (GDPR).

This multi-step process will take time. For example, the process for issuing the adequacy decision for the Privacy Shield framework took six months from the European Commission's proposal in February 2016 to the adoption the adequacy decision in August 2016.

Will the new framework be upheld by the CJEU?

This is the key question. The CJEU has twice invalidated data transfer mechanisms between the EU and United States, the EU-U.S. Safe Harbor Framework in 2015 (the *Schrems I* decision) and the Privacy Shield in *Schrems II,* because of concerns regarding the collection activities of U.S. intelligence agencies and the lack of legal remedies for EU data subjects. Austrian privacy activist, Max Schrems who initiated the legal cases that resulted in both the *Schrems I* and *Schrems II* decisions, has already indicated that he will challenge the TADPF.

One thorny legal issue will be whether EU data subjects have an effective legal mechanism to challenge the U.S. government's collection of their data under the TADPF. Currently, the ability of an EU data subject to obtain judicial redress against the U.S. government regarding its surveillance activities is severely restricted because U.S. surveillance activities are highly secret and EU data subjects must overcome the formidable obstacle of showing they have standing to sue the U.S. government because they have been harmed by these secretive practices.

What do employers need to know?

The key takeaways for EU companies and U.S. companies with employees in the EU are:

- There is no indication that EU regulators will grant a grace period from enforcement activities

while the European Commission undertakes its adequacy decision process to finalize the TADPF. Thus, employers are still required to comply with current EU data transfer requirements by using EU standard contract clauses (SCCs), binding corporate rules (BCRs), or the derogations under the GDPR to transfer EU human resources data to the United States until the TADPF is operational. Employers using SCCs or BCRs must also conduct a transfer impact assessment (TIA) to analyze whether EU human resources data can be safely transferred under current U.S. surveillance laws and whether supplementary technical, contractual or organizational measures must be implemented to adequately protect the transferred data.

- Once the TADPF becomes effective, it will apply only to data transfers from EU/EEA countries to the United States. Data transfers from the UK and Switzerland, which previously recognized the Privacy Shield for transfer of data to the United States, will still need to comply with the UK International Data Transfer Agreement (IDTA) and its version of the TIA, the Transfer Risk Assessment (TRA), or the UK addendum to the SCCs, and the TIA for UK data transfers; and the Swiss addendum to the SCCs and the TIA for Swiss data transfers. Given the expected legal challenges to the TADPF, it is unclear whether the UK or Switzerland will adopt the TADPF to permit data transfers to the United States from their respective countries.

- Similarly, it is unclear at this point whether the TADPF can or will cover onward transfers of human resources data to other third countries like India, such as situations in which a U.S. parent company receives a transfer of human resources data from its EU subsidiary and then transfers this EU data to a payroll company or other vendor in India. Thus, employers may still need to use SCCs and conduct a TIA for such onward transfers.

- Finally, even after the TADPF is operational, employers using the TADPG may wish to continue using the technical, contractual, and organizational supplementary measures under their current SCCs or BCRs in the event that the TADPF is invalidated by a *Schrems III* decision, which, like the *Schrems II* decision, may fail to provide a grace period to find an alternate legal transfer mechanism.

National Law Review, Volumess XII, Number 90