

US and Europe Issue Joint Statement Announcing Agreement on New Trans-Atlantic Data Privacy Framework to Replace EU-US Privacy Shield

WRITTEN BY

Kim Phan | Ronald Raether, Jr. | Angelo A. Stio, III

On March 25, a huge sigh of relief was heard from businesses and organizations located throughout the United States and Europe after the U.S. and European Commission [announced](#) their agreement in principle on a new Trans-Atlantic Data Privacy Framework (Framework) to effectuate the cross-border transfer of personal data from the European Union (EU) to the U.S. After more than a year of discussions, the announcement brings hope that the Framework will alleviate the uncertainty caused by the Court of Justice of the European Union's (CJEU) July 2020 decision in *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties*, Case C-311/18 (Schrems II).

In Schrems II, the CJEU (1) invalidated the EU-U.S. Privacy Shield (Privacy Shield), one of the primary mechanisms utilized for the cross-border transfer of personal data from the EU to the U.S.,^[1] and (2) found that the use of Standard Contractual Clauses (SCCs) to effectuate the cross-border transfer of data were valid, albeit with conditions. Specifically, the CJEU ruled that the Privacy Shield was invalid because Section 702 of the U.S. Foreign Intelligence Surveillance Act and Executive Order 12333 did not limit the public authorities' access to personal data belonging to individuals in the EU. The CJEU also ruled that these laws did not provide EU individuals with effective rights before the courts to challenge access to information by public authorities. In addition, the CJEU found that the use of SCCs was a valid mechanism to effectuate cross-border data transfers, but the CJEU noted that entities relying on SCCs still needed to undertake "assessments" as required by Article 46(1) of the General Data Protection Regulation (GDPR) to safeguard an adequate level of protection to EU individuals.

While no details of the Framework were provided, President Joseph Biden and European Commission President Ursula von der Leyen praised the Framework and reaffirmed their shared commitment to advance privacy, data protection, the rule of law and security. They also noted that the following Framework principles will create:

- A mechanism to ensure that signal intelligence collection will only be undertaken when necessary to advance legitimate national security objectives and not result in a disproportionate impact on individual privacy rights and civil liberties;
- A mechanism to enable EU individuals to seek redress through a multilayer redress program that includes an independent Data Protection Review Court consisting of individuals unaffiliated with the U.S. government who will have full authority to adjudicate claims and direct remedial measures as needed; and

- A requirement for U.S. intelligence agencies to adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

The announcement also indicated that the Framework will continue to require businesses and organizations to comply with the EU-U.S. Privacy Shield principles, including the requirement of self-certification through, and oversight by, the U.S. Department of Commerce. It also indicated that EU individuals will have access to avenues of recourse to resolve complaints against businesses and organizations participating in the Framework.

NYOB, a nonprofit organization founded by Max Schrems, the named litigant in the two prior cases that invalidated prior cross-border data transfer mechanisms ([Schrems I](#) and [Schrems II](#)), issued a statement responding to the announcement. NYOB noted that the announcement was “only a political announcement,” and contained no actual text that could be analyzed. NYOB added that it is not aware of any agreed upon text for the Framework and noted further that the language of the Framework could take months to prepare. NYOB also expressed skepticism about the Framework, questioning how it could pass the essentially equivalent protections test articulated by the CJEU in *Schrems II*. In this regard, NYOB speculates that under the Framework, the U.S. will not change its surveillance laws, but instead, seek to rely on executive reassurances of proportionality for surveillance.

Only time will tell whether the language of the Framework will withstand scrutiny and result in a lawful mechanism to replace the EU-U.S. Privacy Shield and facilitate the cross-border data transfer of personal data from the EU to the U.S. Until the language of the Framework is drafted and disclosed, businesses and organizations will continue to rely on binding corporate rules; standard contractual clauses with protocols for internal risk assessments; maintaining data on servers located in the EU; derogations for specific situations; and utilizing de-identification or anonymization of personal data to address the concerns expressed in *Schrems II*. One thing is certain, both the EU and U.S. recognize the importance of transatlantic data flows to the \$7.3 trillion U.S.-European economic relationship, and they will work toward finding a solution to facilitate these transfers of data.

[1] In July 2020, approximately 5,380 businesses utilized the EU-U.S. Privacy Shield to effectuate the lawful transfer of personal data from the EU to the U.S.

RELATED INDUSTRIES + PRACTICES

- [Privacy + Cyber](#)