May 9, 2022

Guarded Optimism on EU-US Data Transfers: The EU and US Announce Trans-Atlantic Data Privacy Framework

UPDATE August 2023

As of July 17, 2023, another data transfer mechanism became available to many U.S. companies who seek to transfer personal data from the European Union (EU) to the United States. The Department of Commerce announced the availability of the EU-US Data Privacy Framework (DPF) on July 17th, which followed the European Commission's determination on July 10, 2023 that the DPF was adequate for data transfers to the United States. Companies that maintained their Privacy Shield registration have been automatically enrolled in the new framework and will have until October 10, 2023 to update their privacy notices, refresh / confirm their independent dispute resolution mechanism, enter into any necessary onward transfer agreements and continue to perform annual assessments in order to annually re-certify in the framework. Although companies may rely on the DPF to transfer personal data instead of other data transfer mechanisms such as Standard Contractual Clauses (SCCs), it is widely expected that the new framework will be legally challenged and may suffer the same fate as the Safe Harbor and the Privacy Shield programs. Therefore, many companies are continuing to keep the SCCs in place for now or using a belt and suspenders approach by relying on both the SCCs and the new DPF. One benefit to relying on the new DPF, however, is that the European Data Protection Board (EDPB) has noted that supplementary measures are not required if using the DPF whereas such measures must be implemented if relying on SCCs.

The EU and US recently announced that they have reached "an agreement in principle" on a new framework to enable EU-US data transfers following the highly impactful EU ruling that dismantled the prior Privacy Shield framework. European Commission President Ursula von der Leyen made the announcement at a joint press conference with US President Joe Biden, a particularly high profile venue.

Data privacy observers and practitioners are all too familiar with the Court of Justice of the European Union (CJEU)'s (in)famous decision to invalidate the EU-US Privacy Shield in July 2020, in the "*Schrems II*" case. Organizations have spent nearly two years grappling with the implications of the decision, which are still not fully understood, including, many would argue, by the Court itself.

An especially thorny issue the CJEU relied on was the type and degree of government access, via national security surveillance activities, to the personal data being transferred from the EU. The Court determined that the potential for government access resulted in a failure to afford EU data subjects the privacy rights provided by EU law, e.g., the General Data Protection Regulation (GDPR). The Court focused on two sources of authority for surveillance: the Foreign Intelligence Surveillance Act (FISA) Section 702 and Executive Order 12333, which the Court viewed as implicating bulk collection of personal data, without adequate oversight or right to individual redress. As a result, several data protection authorities (DPAs) issued significant orders that certain personal data flows from the EU to the US are unlawful. Many of the recent enforcements result from a series of 101 complaints filed with the EU DPAs by Schrems' advocacy group, noyb. More decisions that further cloud the permissibility of data transfers to the US are expected.

The joint announcement:

The eagerly awaited news of a revised, rehabilitated, or newly created framework for transferring data from the EU to the US arrived in the context of renewed EU-US relations in response to recent geopolitical events, namely, the Russian invasion of Ukraine, as the EU and US announced a plan for a new data transfer framework and increased support for Ukraine.

Von der Leyen framed it as another important means of EU-US cooperation: "Our cooperation on the sanctions against Russia has been exceptional. It shows that when we act together, we are stronger and can make a difference….Pleased that we found an agreement in principle on a new framework for transatlantic data flows. It will enable predictable and trustworthy [EU/US] data flows, balancing security, the right to privacy and data protection."

Early critics focused on the "in principle" qualifier, noting that there are a number of obstacles to the framework becoming reality. Another criticism is that the framework will be immediately subject to litigation – "*Schrems III*" is bandied about in certain virtual hallways. A primary hurdle is that although the framework may be considered to provide adequate protection for EU personal data, the surveillance laws in the US are not likely to undergo material changes that would address the original concerns raised by the Court about the potential overcollection of personal data and national security access by US government. However, the White House indicated that it plans to formalize its commitments in an Executive Order (EO), which is binding law in the US. An EO and Department of Justice (DOJ) regulation will be used to set up a redress mechanism, an extraordinary step toward changing the US legal system in response to EU law.

Transfer mechanisms:

The Privacy Shield, along with other data transfer mechanisms such as standard contractual clauses (SCCs) and Binding Corporate Rules (BCRs) are intended to secure the same level of protection for personal data that the data would receive in the EU.[i] Such measures include data transfer safeguards, e.g., entering into data protection agreements with third parties.

While the initial reaction to *Schrems II* was that it could result in a complete cessation of EU-US data flows, the Court did not actually strike down other cross-border transfer mechanisms, such as SCCs and BCRs, noting that "additional safeguards" might be required to supplement them in order to achieve the desired (if nebulous) level of protection for EU personal data against possible national security government access. In response, the European Commission issued updated SCCs in 2021, nearly a year after the *Schrems II* decision. The model clauses had not been updated since before the GDPR went into effect, and organizations were eager for the updated SCCs to harmonize GDPR transfer obligations and *Schrems II*. While the updated SCCs did not quite achieve this goal, they are an important means of continuing EU-US transfers, with many organizations negotiating additional provisions designed to address the Court's concerns regarding access to data.

Many organizations using Privacy Shield turned to SCCs, and organizations with SCCs in place began the process of making updates to their existing contracts. Organizations using the prior version of the SCCs had until September 27, 2021 to start using the new SCCs for all new (or modified) data transfers and will have until December 27, 2022 to replace the prior SCCs currently in effect. See our recent alert for more on updating privacy contracts.

Negotiating a new framework:

Following the *Schrems II* decision, high level EU and US negotiators began discussions for a cross-border transfer solution to replace Privacy Shield. For months, there were whispers of progress, and at times, what seemed to be major impasses to any agreement.

The announcement was vague, although the EU and White House have since released some information related to what might be included in the framework:

- The ability for EU persons to seek redress from perceived unlawful targeting by signals intelligence activities, including the formation of an independent Data Protection Review Court composed of people from outside US government.
- A US commitment "to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives."
- Enhancements to the existing oversight of US intelligence agencies for "new privacy and civil liberties standards."

The language of these commitments reflects a nod to the treatment of privacy as a fundamental right under European law. They also reflect an adherence to the specific, distinct concerns of the CJEU. However, the details give rise to further questions – e.g., signals intelligence (SIGINT) activities are already subject to rigorous oversight and a legal process designed to limit data collection – what might these new safeguards entail? And would they be sufficient to ward off the inevitable legal challenges?

Reactions to the announcement:

The financial implications of EU-US data transfers loom large in the efforts for a new framework. As noted in the White House statement, "the deal will enable the continued flow of data that underpins more than $1 trillion in cross-border commerce every year." As such, the announcement was largely welcomed by the business community, particularly the tech industry, but found mixed reactions from international lawyers, advocacy groups, and others with close involvement with the privacy and security-based legal issues critical to the success or failure of a new transfer mechanism.

The reactions range from glowing praise to harsh criticism. Google issued a statement commending the EC and US, stressing that "Google has long advocated reasonable limits on government surveillance." The EDPB released a statement, noting that it would "examine how this political agreement translates into concrete legal proposals to address the concerns raised by the Court of Justice of the European Union (CJEU) in order to provide legal certainty to EEA individuals and exporters of data." As anticipated, Max Schrems responded to the announcement with skepticism, via tweet and a statement through his advocacy group (noyb) saying that he would have liked the US and EU to come to a "no spy" agreement. Many critics of the deal attack it because it relies on Executive action without statutory force, but the negotiators emphasize that what they could get out of

Congress (even prior to the US midterm elections) would be substantively so much weaker that action by the Administration is the only viable approach.

European data protection authorities (DPAs) also began weighing in, and it will be important to monitor their positions regarding enforcement.

Looking forward (or across the pond):

Before the framework is finalized, the DPAs could issue additional enforcements on EU-US transfers. It is possible that the regulators could suspend enforcements in the interim, as they did with Privacy Shield.

In order for the trans-Atlantic data privacy framework to move from an "in principle" political agreement to an effective, viable data transfer mechanism, it must navigate a series of EU legal and legislative obstacles, and establish that the framework is *adequate* to protect EU personal data. First, the European Commission (EC) will conduct an adequacy analysis and draft an adequacy determination for the European Data Protection Board (EDPB). The EDPB will issue an opinion, to which the EC is not bound. However, the EC may revise its draft decision based on feedback and opinions of the EDPB, European Parliament (EP), Council of Europe, and others – although it is not expected to make substantial changes. The EP may also adopt a non-binding resolution. Next, the Member States must approve the framework by a 55% majority. Finally, the EC College of Commissioners would formally adopt the decision, which would take effect upon publication in the EU Official Journal. The process is expected to take several months at least.[ii] On the US side, the commitments will be included in an Executive Order.

Critics of the CJEU opinion rightfully argue that the adequacy standard itself, is particularly misleading, as various EU countries (and other countries around the world) allow for an even greater degree of surveillance of foreign and domestic persons, often with less oversight, transparency, and legal process than the US. However, the wording of the decision of the Court is what the negotiators had to take into consideration, and without the ability to unilaterally alter US surveillance laws, the new framework is sure to face immediate challenge.

While the criticism is duly warranted, the Trans-Atlantic Privacy Framework announcement signifies a major step toward a new US-EU data transfer mechanism and a high-profile venue was deliberately chosen for doing so. The negotiations between the US and EU are now entirely over, and while the text could change based on the approval process, there will be no more negotiations – leaving questions mainly as to the wording of the EO on the US side and review and approvals on the EU side.

We now await the substantive terms of the deal – and the one thing most observers agree upon is that the (legal) devil will be in the details – both as an implementable data transfer solution and as a framework that will hold up to the next challenge in the EU legal system. For now, "in principle" is what we get.

While we await the finalization of the Trans-Atlantic Privacy Framework, there are some actions organizations should take:

- Review data transfer/protection agreements and SCCs and implement new SCCs by the December 2022 deadline.
- Evaluate, document, and where necessary, implement "additional safeguards" for cross-border data transfers.
- If your organization has certified to the Privacy Shield, continue to adhere to Privacy Shield obligations as the new deal is finalized.
- Complete transfer impact assessments (TIAs) for personal data transfers out of the EU/UK. When issued, include the new Executive Orders and DOJ regulation in TIAs.
- Consider preparing playbooks and/or engaging outside attorneys to help negotiate data protection agreements on behalf of your organization.
- Look for additional guidance from the EU regulators as to whether or how they plan to enforce data transfers in the meantime; different regulators are likely to take different approaches.

Footnotes

---

[i] For the purposes of this article, the EU will collectively be used to refer to the EU member states, although the same data protection arguments apply to Switzerland.

[ii] See IAPP, *From Privacy Shield to the Trans-Atlantic Data Privacy Framework*, April 2022 for a timeline of the EU approval process described in this paragraph.