The Data Privacy Framework has Landed! How to Reap the Benefits - A Blog Post by Michael Whitener

The long-awaited successor to the Privacy Shield has finally arrived. Like the Privacy Shield, the new program, dubbed the *Data Privacy Framework* (DPF), provides for a self-certification process allowing U.S. companies to receive transfers of personal data from the European Union, the United Kingdom and Switzerland.

The DPF emerged from three recent political developments:

1. An "agreement in principle" (in March 2022) between the European Union and the United States on a mechanism to allow transfers of EU personal data to the United States.
2. President Biden's issuance (in October 2022) of Executive Order 14086, which imposes new guardrails around U.S. government surveillance activities and new redress options for individuals who believe their data has been unlawfully obtained by U.S. government authorities.
3. The European Commission's adoption (in July 2023) of an "adequacy decision" concluding that, under the DPF, the United States ensures an adequate level of protection for EU personal data transferred to U.S. companies.

Some brief history for context. From 2009 until 2015, the Safe Harbor Framework permitted the free flow of EU personal data to Safe Harbor-certified companies in the U.S. In 2015, however, the Court of Justice of the European Union (CJEU) invalidated Safe Harbor on the basis that it didn't protect EU personal data in ways "essentially equivalent" to those provided by the EU Data Protection Directive (succeeded in 2018 by the GDPR).

In 2016, the Privacy Shield was approved to replace Safe Harbor, with significantly stronger privacy protections, oversight mechanisms and redress options. The Privacy Shield unfortunately suffered the same fate as Safe Harbor at the hands of the CJEU (in its 2020 *Schrems II* decision), although specifically on grounds relating to U.S. government surveillance activities. (The standard contractual clauses (SCCs) survived CJEU scrutiny, but SCCs are a more cumbersome data transfer mechanism, even after being updated with a modular structure in 2021.)

The Biden Administration's EO 14086 was aimed squarely at addressing the concerns raised in *Schrems II* – and the European Commission agreed it had successfully done so. That paved the way for final DPF approval.

How to Become DPF Certified

Now for the practical part. How can U.S. companies take advantage of the DPF? There are two different paths, depending on whether a company had previously self-certified under the Privacy Shield.

1. **Privacy Shield Certified Companies**

If your company self-certified to the Privacy Shield and has maintained its Privacy Shield certification (despite the Privacy Shield being a dead letter for data transfers since *Schrems II*), you're in luck: Privacy Shield participants have essentially been waived into the DPF. On the U.S. Commerce Department's new DPF website, active Privacy Shield participants have been converted to DPF participants, including both the EU-U.S. DPF and (assuming a company previously certified under the Swiss-U.S. Privacy Shield) the Swiss-U.S. DPF. The next annual re-certification due dates remain the same as under the Privacy Shield.

For data transfers from the United Kingdom, given the UK's exit from the EU in 2020, there is now an additional step to take: affirmatively opting in to certification under the UK Extension to the EU-U.S. DPF. This additional certification is based on a "data bridge" agreed between the U.S. and the UK that will connect the UK to the EU-U.S. DPF.

With regard to data transfers from the UK and Switzerland, there's one twist to be aware of. While previously Privacy Shield-certified companies may immediately begin relying on the EU-U.S. DPF for personal data transfers from the European Economic Area (which includes not only EU countries but also Iceland, Liechtenstein and Norway), they may not yet do so under the UK Extension or the Swiss-U.S. DPF. The UK and Switzerland must take additional measures (still pending) to formalize their participation in the DPF.

The final requirement for previously Privacy Shield-certified companies is to update their privacy policies to comply with the DPF (with a three-month grace period to do so). The Commerce Department has drafted very helpful sample language for inclusion in DPF-compliant privacy policies, including (i) how to refer to your participation in the DPF program, and (ii) how to inform individuals about your company's methods of dealing with any complaints concerning your handling of their personal data under the DPF, including their rights to resort to an "independent recourse mechanism."

Note that if your independent recourse mechanism under the Privacy Shield was a Commerce Department-certified organization such as the International Centre for Dispute Resolution (a division of the American Arbitration Association) or JAMS, those organizations are certified under the DPF as well.

If your company was previously Privacy Shield-certified but does *not* wish to participate in the DPF, there is a formal withdrawal procedure. Doing nothing isn't an option.

2. **Non-Privacy Shield Certified Companies**

If your company was *not* Privacy Shield certified (i.e., you never certified in the first place or you withdrew from the Privacy Shield), the DPF certification requirements are quite similar to those of the Privacy Shield:

- *Develop a DPF-compliant privacy policy.* In the privacy policy, the company must commit to conforming with the DPF Principles, and the privacy policy must include all of the elements required under the Notice Principle.
- *Select an independent recourse mechanism.* This mechanism could be a private-sector dispute resolution body or a European data protection authority.
- *Put in place a DPF verification method.* Your company must have procedures in place for verifying that the DPF attestations are true and that your privacy policy has been implemented in accordance with the DPF Principles. Options are either self-assessment or verification using a third-party service.
- *Designate a company contact.* Your company must provide a contact for the handling of complaints, access requests and other DPF compliance issues.
- *Submit self-certification to the U.S. International Trade Administration (ITA).* The DPF program website provides a straightforward process for submitting all the information required for DPF certification. A self-certification processing fee must be paid, based on an organization's annual revenues (starting at $375 for annual revenues of up to $5 million if a company elects to participate in both the EU-U.S. DPF and the Swiss-U.S. DPF).

Once the self-certification request is submitted, the ITA will review to ensure the submission meets all DPF requirements. The ITA will notify your company if any deficiencies are identified. When the self-certification is approved, the ITA will notify your company by email.

Will the DPF Survive Legal Challenge?

The DPF inevitably will face legal challenges, as did the Privacy Shield and Safe Harbor before it. In particular, Max Schrems and his organization NOYB, which brought the claim that resulted in the Privacy Shield's demise in the *Schrems II* decision, has promised that there will be a *Schrems III*.

Nevertheless, there is good reason to be optimistic that any lawsuits will be beaten back, given three significant improvements of the DPF over the Privacy Shield:

1. *Limitations on U.S. government access.* EO 14086 significantly reins in the rights of U.S. intelligence agencies to conduct surveillance involving access to EU personal data. In particular, EO 14086 requires that surveillance activity be necessary for a "validated intelligence priority" and only be used when less intrusive methods aren't feasible.
2. *Additional redress methods.* The DPF adds several new avenues by which EU residents can seek to get their privacy complaints resolved. In particular, under EO 14086, a new Data Protection Review Court will be responsible for investigating and resolving complaints from EU residents regarding access to their data by U.S. intelligence agencies.
3. *Greater transparency.* The DPF mandates an annual review of both the redress process and whether U.S. intelligence agencies have complied with the new limitations established by the DPF and EO 14086.

* * *

The DPF provides a welcome alternative to SCCs for facilitating data flows from Europe to the United States. Considering that Europe is the United States' largest trading partner, with the value of transatlantic commerce exceeding $1 trillion annually, the DPF's advent is worth celebrating.

Please let us know if we can assist with your DPF certification, including by updating your privacy policy to meet DPF requirements, incorporating DPF terms into your data processing agreements, or otherwise advising on DPF compliance.