Weathering the Storm of Transatlantic Data Regulations

Janice F. Mulligan
Mulligan Law
Lexing Network
US California Affiliate

The GDPR restricts the transfer of personal information (PI) out of European Union Member States unless the recipient is in another Member State or a country with an "adequate" level of protection. The EU–US Data Privacy Framework of 2022 (DPF) is a recently enacted data transfer policy designed to comply with the GDPR in the transatlantic exchange of PI. Previous agreements, including the EU–US Privacy Shield (2016–2020) and the International Safe Harbor Privacy Principles (2000–2015), were both stricken down by the European Court of Justice on the grounds that personal EU data was subject to sweeping US government surveillance that didn't protect Europeans' PI privacy rights.[i]

Since the EU–US Privacy Shield was voided in July 2020, companies transferring data between the EU and the US "faced confusion, higher compliance costs, and challenges for EU–US business relationships".[ii] Fortunately, some help is on the way.

Despite the lack of any comprehensive US federal laws to protect PI, the current DPF purports to address these EU privacy concerns. In October 2022, US President Joe Biden signed an executive order restricting US federal intelligence surveillance use of spyware, and creating a process for individuals to seek redress of claims that PI collected through US signals intelligence was collected or handled by the US in violation of American law.[iii]

The goal of issuing this executive order was to obtain an "adequacy decision" from the European Commission which would allow the lawful transatlantic flow of PI to the United States for commercial purposes. Under Article 45(1) of the GDPR, such cross-border data transfers are permitted if the country has an adequate level of protection demonstrated by receipt of an "adequacy decision."

In May 2023, the European Parliament voted in favor of a resolution calling on the Commission ***not to adopt*** an adequacy finding because "the EU–US Data Privacy Framework [DPF] *fails* to create essential equivalence in the level of protection".[iv] This Parliamentary decision was not binding on the European Commission.

Despite this Parliamentary resolution, in July 2023, the European Commission adopted an adequacy decision ***in favor of*** the United States based on the DPF. This adequacy decision will allow the commercial transfer of data with the United States and the EU, Switzerland, England and Gibraltar (pending the latter countries' formal approval.)[v] [vi]This EU decision imposes limitations on access to data by intelligence *and law enforcement agencies*, and establishes an independent and impartial mechanism to handle complaints from European citizens relating to the collection of their data for alleged national security purposes.[vii] Note that the US executive order which this decision was based on *did not and could not promise restrictions on American state and local law enforcement agencies, because these are governed primarily by state and not federal law.* The US executive order does however apply to US federal surveillance activities.[viii]

How does all of this affect the commercial transatlantic transfer of PI? Many companies will now have choices regarding how they choose to proceed with the transatlantic flow of PI. These choices are described below:

VOLUNTARY SELF-CERTIFICATION UNDER THE DPF:

The US International Trade Administration launched a DPF website that includes information on *voluntary* self-certification for U.S. based organizations, and US subsidiaries of foreign corporations.[ix] The website also contains a list of all U.S. companies that have obtained voluntary certification under the DPF. In the first month that the certification process was available, over 2800 U.S. companies obtained voluntary certification.

These participating companies are deemed to provide "adequate" data privacy protection, thus satisfying the requirement for the transfer of personal data outside of Europe. Because adequate protection is provided by certified companies, contracts with such organizations for processing of data will *not* require prior authorization.

Does this sound too good to be true? The devil is in the details. While this certification is voluntary, thoughtful planning should be made before companies rush to seek compliance under the new framework. Why? Because while the decision by an eligible U.S.-based organization to self-certify its compliance and

participate in the DPF program is *voluntary*, once self-certification is completed, **compliance is *compulsory,* and enforceable under US law.**

What will participating companies be required to do to obtain voluntary certification? The reader is directed to review the website cited at endnote xi below for the numerous requirements, some of which include:

1. **Inform individuals about data processing**
    a. A declaration of the company's commitment to comply with the DPF Principles is required so that the commitment becomes enforceable under US law.
    b. The company must inform individuals of their right to access personal data; disclose personal information in response to lawful requests by public authorities; and, disclose the participating company will be liable in cases of unauthorized transfer of data to third parties.

2. **Provide free and accessible dispute resolution**
    a. The company must respond to any individual complaints within 45 days.
    b. *At no cost to the individual*, participating organizations must provide an independent recourse mechanism for dispute resolution. The website identifies multiple mediation/arbitration services, any one of which can meet this requirement.
    c. If an individual submits a complaint to a data protection authority (DPA) in Europe, the company commits to receive, review and undertake best efforts to facilitate resolution of the complaint and to respond to the DPA within 90 days.
    d. Participating companies must *commit to binding arbitration* at the request of the individual to address any complaint that has not been resolved by other mechanisms.

3. **Maintain data integrity and purpose limitation**
    a. Participating companies must limit PI to the information relevant for the purposes of processing.
    b. Participating companies must comply with the data retention provision.

4. **Ensure accountability for data transferred to third parties**

To transfer personal information to a third party acting as a controller, or to any third party acting as an agent, a participating organization must:

a. Comply with the Notice and Choice Principles; and
b. The third-party controller or agent must contractually agree that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual; that the recipient will provide the protection required by the DPF Principles; and will notify the company if it decides that it can no longer meet this obligation. When such a determination is made, the third-party controller or agent ceases processing or takes other appropriate steps to remediate.

5. **Commit to transparency in any enforcement actions:**
   If the company becomes subject to an FTC or court order based on non-compliance, the company must make public any relevant DPF-related compliance or assessment reports.

6. **Ensure commitments are kept as long as data is held**
   If a company leaves the DPF program, it must annually affirm its commitment to apply the DPF Principles to information received under the DPF program if it chooses to keep such data; otherwise, it must provide "adequate" protection for the information by another authorized means.

ALTERNATIVES TO VOLUNTARY CERTIFICATION WITH THE DPF: "SCCs" and "BCRs"

What is a company to do if it either doesn't qualify for, or elects not to seek, voluntary certification under the DPF?

The *Schrems II*[x] decision invalidated the Privacy Shield, and called into question data transfers using standard contractual clauses (SCCs). SCCs are standardized and pre-approved model data protection clauses that can be incorporated into contracts, allowing the parties to comply with their GDPR obligations. [xi] The repeal of the EU-US Privacy Shield severely limited previous GDPR contractual methods for transferring EU PI across the Atlantic.

In response to the lack of confidence placed on SCCs following the Schrems II decision, in June 2021, the European Commission adopted a new set of SCCs,[xii] for the transfer of personal data to countries outside of the European Economic Area (EEA)[xiii]. They contain specific data protection safeguards to ensure that PI has a "high level of protection" when transferred outside the EEA. They can be used by data exporters, *without the need to obtain a prior authorization from a data protection authority*. By adhering to the SCCs, data importers contractually commit to abide by a set of data protection safeguards.

As an alternative to SCCs, another method of transferring data to the United States includes inter-company transfers, based on Binding Corporate Rules (BCR). BCRs are typically used by multinational organizations that make frequent intracompany cross-border transfers. These rules are created by the company and then reviewed and approved through the local Data Protection Authority (DPA) in accordance with GDPR, Article 63. The European Data Protection Board (EDPB), issues a final opinion before final approval by the DPA.[xiv]

CONCLUSION

Given the United States' continued failure to have a comprehensive set of federal laws to safeguard PI, it remains unclear as to how the DPF will fare in the European Court of Justice. *For now*, companies trying to comply with ever-changing and often contradictory international regulations face smoother seas, but should be concerned that this may be just a respite before yet another transatlantic data regulation storm.

---

[i] *Schrems v. Data Protection Commissioner*, Case C-362/14 6 October 2015 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 ("Schrems I") and Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18 16 July 2020 https://curia.europa.eu/juris/liste.jsf?num=C-311/18 ("Schrems II") Retrieved August 16, 2023

ii *"Legal Questions Loom Over Latest Trans-Atlantic Data Flows Deal"*. news.bloomberglaw.com. Retrieved August 17, 2023.

[iii] *Biden Signs an Executive Order on EU-US Data Privacy Agreement, 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/* Retrieved August 16,2023

[iv] "Texts adopted – Adequacy of the protection afforded by the EU-US Data Privacy Framework". European Parliament. 11 May 2023. Retrieved August 17, 2023

[v] Separate agreements were entered into for the EU-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US DPF, and the Swiss-US Data Privacy Framework (Swiss-US DPF).

[vi] All Member States of the European Union are bound by the European Commission's adequacy decision for the EU-US DPF, the United Kingdom and Gibraltar will be bound by the UK Government's data bridge for the UK

Extension to the EU-US DPF, and Switzerland will be bound by the Swiss Federal Administration's recognition of adequacy for the Swiss-US DPF once those government actions enter into force.

[vii] *Adequacy decision for the EU-Data Privacy Framework" https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en* Retrieved August 16, 2023.

[viii] *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* involves data transfers for law enforcement purposes and it is not affected by the DPF.

[ix] *Data Privacy Framework Program*, US Department of Commerce International Trade Administration (ITA) https://www.dataprivacyframework.gov/s/data-protection-authorities Retrieved August 16, 2023.

[x] See Footnote I above.

[xi] *European Commission New Standard contractual Clauses- Questions and Answers Overview* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en Retrieved August 16, 2023

[xii] *Standard contractual clauses for international transfers*, https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en Retrieved August 16, 2023

[xiii] The European Economic Area (EEA), is comprised of the 27 Member States of the EU as well as Iceland, Liechtenstein and Norway.

[xiv] *Binding Corporate Rules (BCR): Corporate rules for data Transfer Within multinational companies https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en* Retrieved August 16, 2023