EU-U.S. Privacy Shield—Recent Challenges: Impact on the U.S. and What Businesses Need to Know

By Aaron Charfoos and Erin Fonté

Your company, like many others, transfers personal data on European citizens from Europe to the U.S. But, are you doing it properly? There has been a lot of talk about the new European Union-U.S. data transfer agreement, Privacy Shield, that has been in place for four months now. What is the Privacy Shield, is it right for your company and what are your other options? This article takes a look at what Privacy Shield is, the practical implications of relying on Privacy Shield and other data transfer options and helps you choose the right option for your company.

Why You Cannot Just Transfer Personal Data Outside the EEA

In April 2016 the EU adopted the General Data Protection Regulation (GDPR). The GDPR replaces a more decentralized privacy statute, known as the Data Protection Directive, that has been in place since 1995 with a comprehensive, mostly 'one-stop shop' for privacy rules. The GDPR, like its predecessor has provisions intended to give businesses uniform national laws to comply with. The GDPR also requires high standards of data protection in cross border transfers of personal data from the EU to countries outside of the EEA.
Despite all of the challenges facing Privacy Shield, there are some very good reasons to use it as the legal mechanism to transfer your personal data.

Proper EEA Data Transfer Mechanisms

There are predominantly four mechanisms to transfer EEA to the U.S. enterprises may use to transfer personal data from the EEA to the U.S.:

- **Standard Contractual Clauses**: U.S. companies may enter into a form of model clauses approved by the European Commission for data transfers.
- **Binding Corporate Rules (BCRs)**: For enterprises that rely on significant intra-group transfers, the European Commission has encouraged the use of BCRs. These are a single set of binding, enforceable rules applied across entities of a corporate group that have been submitted to, and approved by, the European Commission. Properly implemented, these may permit a U.S. enterprise to rely on an alternate legal mechanism to transfer the data.
- **Consent and other exceptions**: There are also several exceptions to the prohibition on transfer of data, including if the data subject "has unambiguously given his/her consent to the proposed transfer" and, in certain instances, when it is necessary for the performance of a contract between the data subject and an enterprise.

The first step is to fully understand what personal data or sensitive data collected, here it used, has it been transferred outside of the U.S. and how is it processed with other information to identify legal means of protecting personal data. In addition, you can determine the best way to transfer the information from the EEA to the U.S.

Privacy Shield

Despite all of the challenges facing Privacy Shield, there are some very good reasons to use it as the legal mechanism to transfer personal data. Contracts do not land Privacy Shield in front of the European Court of Justice who could invalidate the agreement. Given this uncertainty, should your agreement again. Given this uncertainty, should your agreement again. Given this uncertainty, should your agreement again. Given this uncertainty, should your agreement again.

One of the common elements under both the 2016 EU Data Protection Directive and GDPR is that companies can only transport personal data out of the EEA to a country that the EU has previously declared to be "adequate" for data protection laws. While countries such as Argentina, Brazil, and South Africa have been deemed adequate, the EU has refused to find the current U.S. system adequate. Therefore, to transfer personal data of EEA citizens to the U.S. enterprises may rely on significant intra-group transfers, the European Commission has encouraged the use of BCRs. These are a single set of binding, enforceable rules applied across various entities of a corporate group that have been submitted to, and approved by, the European Commission. Properly implemented, these may permit a U.S. enterprise to rely on an alternate legal mechanism to transfer the data.

The first step is to fully understand what personal data or sensitive data has been collected, how it used, has it been transferred outside of the U.S. and how is it processed with other information to identify legal means of protecting personal data. In addition, you can determine the best way to transfer the information from the EEA to the U.S.

Privacy Shield

Despite all of the challenges facing Privacy Shield, there are some very good reasons to use it as the legal mechanism to transfer personal data. Contracts do not land Privacy Shield in front of the European Court of Justice who could invalidate the agreement. Given this uncertainty, should your agreement again. Given this uncertainty, should your agreement again. Given this uncertainty, should your agreement again.
Although at least one nongovernmental privacy group privately (which is both good and bad), governmental entity, they can simply be entered into privacy agreements—or BCRs, as they are referred to by the European Union—between two separate legal entities (all connected by one parent company). These agreements can be instantaneously approved by the relevant EU DPAs, and every entity within the corporate structure (who will be receiving the information) must agree to the terms of the BCRs. The BCRs are then submitted to all of the relevant EU DPAs who must then approve the BCRs. These agreements and policies will be found unacceptable in a future enforcement proceeding.

Binding Corporate Rules

If you are a large, multinational corporation that handles large amounts of sensitive personal information (for example, medical information), then you might want to consider adopting Binding Corporate Rules. There are two main types of Binding Corporate Rules, one for Controller to Processor transfers and one for Processor to Processor transfers. These are binding, much as Standard Contractual Clauses, and the DPAs are not required to re-evaluate them on an ongoing basis. As such, they are relatively straightforward, the steps the company needs to take to protect the data here in the U.S. are well-defined and if approved, the company can publicly promote the fact that it has a transfer mechanism in accordance with the U.S. government (assuming that the company continues to follow the required steps).

Privacy Shield is best suited for companies that will be sending a modest amount of data from the European Economic Area to the U.S. only. In contrast, Binding Corporate Rules can accommodate far more. Although they only require the company to ship a product and then give notice the EEA citizen upon delivery, the company may have a very different definition. Consent is best suited to companies who handle large amounts of sensitive personal information then you might want to consider adopting Binding Corporate Rules.

Consent and Exceptions

There are several other ways to legally transfer personal data out of the EEA. First, a company can seek the consent of the data subject to transfer the data outside of the EEA. Consent is a defined term in the GDPR, requiring, 'freely given, specific, informed and unambiguous indication of the data subject’s wishes . . .’ Therefore, opting-out will not satisfy the GDPR's requirements. So, for companies who want to consider adopting an exception to the GDPR, such as nonprofits, depository institutions or insurance companies, may not be eligible for Privacy Shield so it is important to consult counsel on its availability.

Standard Contractual Clauses

Under the current EU Directive, and under Article 46 of the GDPR, companies may rely on Standard Contractual Clauses to transfer personal information out of the EEA. There are two Standard Contractual Clauses, one for Controller to Processor data transfers and one for Controller to Controller data transfers. These Standard Contractual Clauses are essentially form contracts, rather than custom agreements. The Clauses are best suited for larger organizations that need to regularly transfer personal information and why it is being transferred.

The Clauses are essentially a pre-negotiated form contract that can be easily used by both parties to the contract. The Clauses are available on the European Commission’s website and are relatively straightforward. Companies that want to use the Clauses must simply fill out an online form and submit the information to the relevant EU DPA. The DPA will then evaluate the Clauses and approve them if they meet the requirements of the GDPR. If the Clauses are approved, the company can publicly promote the fact that its data transfer mechanism is well defined and, if approved, the company can publicly promote the fact that its data transfer mechanism is sanctioned by the U.S. government (assuming that the U.S. can conduct and will give EEA citizens the same rights to challenge that surveillance as U.S. citizens. Moreover, just after the election win for President-Elect Trump, certain DPAs stated that they did not believe that his election would endanger the protections in place under the GDPR, and the fact that no BCRs had been approved yet, thus it is likely to remain valid for the foreseeable future.

Privacy Shield is best suited for companies that will be sending a modest amount of data from the European Economic Area to the U.S. only. It imposes a challenge to Standard Contractual Clauses, given that several companies have gotten transfer mechanism under the GDPR, and the fact that no BCRs had been approved yet, thus it is likely to remain valid for the foreseeable future.
Choose Wisely

There are a number of mechanisms that companies must use to legally transfer personal data out of the EEA to the United States. However, the risks of improperly transferring the data are huge. The GDPR provides for fines up to the greater of 20 million euros ($22.1 million) or 4 percent of global revenue. It is not enough to simply choose a transfer mechanism, put it up on the shelf and then forget about it. Companies must make sure they are not only complying with the requirements of the transfer mechanism but also still have the right mechanism in place as their business model and service offerings evolve over time. The risks are simply too great to get this wrong.