Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 12 >>> DECEMBER 2016

European Union

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

By Aaron Charfoos and Erin Fonté

Aaron Charfoos is a member in Dykema's Privacy, Data Security and E-Commerce practice in Chicago and is an experienced trial lawyer specializing in complex privacy and data protection litigation and counseling.

Erin Fonté is a member in Dykema's Privacy, Data Security and E-Commerce practice in Austin, Texas and specializes in a broad range of matters related to payments/payment systems, digital commerce, banking and financial services.

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 scheme, known as the Privacy Directive, that has been in place since 1995 with a comprehensive, mostly "one-stop shop" for privacy rules. The GDPR, like its predecessor law, protects "personal

data" of any European Economic Area (EEA) citizen. Personal data is broadly defined to include "any information relating to an identified or identifiable natural person." Moreover, the GDPR will apply to any company "offering goods or services" in the EEA regardless of whether the company is headquartered in Europe, giving the GDPR extra-territorial reach. Many companies also overlook the fact that the GDPR protects the personal data of not only their customers and clients, but also their own employees. The GDPR, will become effective in May 2018.

One of the common elements under both the 1995 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 has "adequate" data protection laws. While countries such as Argentina, Iceland and Israel have been deemed adequate, the EU has refused to find the current U.S. system adequate. Therefore, companies cannot simply transfer personal data of EEA citizens from Europe to the U.S. Instead, they need to rely on an alternate legal mechanism to transfer the data.

For the past 15 years, the U.S.-EU Safe Harbor, a bilateral agreement between the EU and U.S. allowed thousands of U.S. businesses to move information from the EEA to the U.S. if they had self-certified with the U.S. Department of Commerce. However, in Oct. 2015 the European Court of Justice struck down Safe Harbor, saying it did not adequately protect the rights of EEA citizens.

In the wake of this decision, European Union and U.S. negotiators crafted a new framework, called the EU-U.S. Privacy Shield, which came into force in Aug. 2016. Like the prior Safe Harbor, the framework governs the steps a U.S. organization needs to take in order to ensure that any data moving out of the EU is properly protected once it lands in the U.S. The Privacy Shield once again relies on self-certification, but is far more stringent in terms of notice, consent, recertification, adopting efficient mechanisms to raise privacy concerns by EU citizens and oversight by relevant U.S. governmental agencies. In addition, the Privacy Shield addresses concerns about surveillance by the U.S. government itself.

Privacy Shield still faces an uncertain future, however. Although the EU Article 29 Working Party, a committee of EU governmental Data Protection Authorities (DPA), have agreed not to file any challenges to Privacy Shield until at least August 2017, numerous private organizations have filed legal challenges in member state and national forums. This could land Privacy Shield in front of the European Court of Justice who could invalidate the agreement again. Given this uncertainty, should your company rely on Privacy Shield? And what are the other options?

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 citizen's personal data from the EEA to the U.S.:

- **Privacy Shield**
- **Standard Contractual Clauses:** U.S. enterprises may enter into one of the forms of model clauses approved by the European Commission for data transfer.
- **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 various entities of a corporate group that have been submitted to, and approved by, European DPAs. Given their complexity and long approval process, these are most appropriate for large, multinational enterprises.
- **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 the enterprise.

The first step is to fully understand what personal data or sensitive data is collected, how it is used, how it is protected, with whom it is shared, how long it is kept and where it is stored and moved. Once you have done that, 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 your personal data. To begin with, the legal challenges to Privacy Shield are not necessarily going to bring down the agreement like Safe Harbor. Before the European Court of Justice's opinion striking down Safe Harbor, many people felt that the 15 year old law did not adequately address the privacy concerns of today. Therefore, the U.S. and EU had already been renegotiating Safe Harbor 2.0. The *Schrems* case, which invalidated Safe Harbor, hastened Safe Harbor's demise, but many people were looking to replace it in any event. Negotiators had this background, and the ECJ's opinion, in mind as they worked on Privacy Shield. That agreement went through many layers of U.S. and European review, had the backing of many EU politicians and was tentatively supported by the committee of European Data Protection Authorities post *Schrems*.

  WDPR ISSN 1473-3579

Recent developments will also help support the viability of Privacy Shield. One of the biggest privacy concerns is whether the Privacy Shield will adequately protect against surveillance by the U.S. government. The U.S. and EU appear to be ready to sign an umbrella agreement that will provide guidance on what surveillance 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 included within Privacy Shield.

So what kinds of companies should consider certification under Privacy Shield? Privacy Shield is best suited for companies that will be sending a modest amount of data from the EEA to the U.S. only—not larger multinational companies who may be sending the data to multiple locations or sending the data on to third parties after it arrives in the U.S. Additionally, some companies, 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.

The benefits of using Privacy Shield are that the application is 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 its data transfer mechanism is sanctioned by 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.

Standard Contractual Clauses

Under the current EU Directive, and under Article 46 of the GDPR, companies may rely on Standard Contractual Clauses to transfer personally identifiable information out of the EEA. There are two Standard Contractual Clauses, one for Controller to Controller data transfers and one for Controller to Processor transfers. These Standard Contractual Clauses are essentially form contracts that have been approved by the EU and that are entered into between two separate legal entities (although they are often part of a larger related corporate structure). The Clauses do not allow for any room to modify the actual terms of the agreement, only to set out the kinds of data transferred, what entities will transfer the data and why it is being transferred.

The Clauses are best suited for larger organizations that are transferring data between a number of corporate entities or if the data transfers will be out of the EEA to a number of different companies—not just those in the U.S. They do not necessarily require approval of any governmental entity, they can simply be entered into privately (which is both good and bad).

Although at least one nongovernmental privacy group has filed a challenge to Standard Contractual Clauses, given their recent adoption as proper transfer mechanisms under the GDPR, and the fact that no DPA challenged their legality, they are likely to remain valid for the foreseeable future.

Similarly, companies may enter into *ad hoc* contracts or agreements that would adequately protect the privacy of the personal data. However, without the preapproval of a governmental authority, companies run the risk that those agreements and policies will be found inadequate 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. The adoption and approval process is long and expensive – so much so that less than 100 companies have adopted BCRs so far. Essentially the corporation creates a set of corporate rules and regulations regarding the use, transfer and protection of personal information. Each 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. BCRs remain the gold standard for legal data transfers. However, it is a unique company that puts them in place.

If you are a large, multinational corporation that handles 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 may seek the consent of the data subject to transfer their information. "Consent" is a defined term in the GDPR requiring, "freely given, specific, informed and unambiguous indication of the data subject's wishes . . ." Therefore, opt-outs and fine print contracts that may be permitted here in the U.S. are unlikely to pass muster under this stringent definition. Consent is best suited to companies who may have EEA clients or customers, but do not have an office or related corporate entity in Europe or who transfer a very small amount of data overseas.

Finally, companies may legally transfer data if it is in the furtherance of a contract with the data subject. So, for example, if you have a contract with a EEA citizen that requires the company to ship a product and then give notice the EEA citizen upon delivery, the company may transfer the contact information of the citizen in order to effectively provide that notice. However, companies should be careful that the transfer must truly be furtherance of the contract—not for other, ancillary purposes like marketing related products or services to the client.

Choose Wisely

There are a number of mechanisms that companies may use to legally transfer personal data out of the EEA to the U.S. However, the risks of improperly transferring the data are huge. The GDPR provides for fines up to the greater of 20 million euros ($ 20.8 million) or 4 percent of global revenue. It also is not enough to simply chose a transfer mechanism, put it up on the shelf and then forget about it. Companies must ensure that 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.

   ISSN 1473-3579