ABA Section of International Law
Your Gateway to International Practice
EUROPE UPDATE
DATA PRIVACY EDITION
Issue 25, February 2018

Privacy Law: Europe's Impact on US Business

EU-US Privacy Shield: Will It Shield You from the General Data Protection Regulation (GDPR)?

by

Aaron Schildhaus, Counsel, Scharf Banks Marmor LLC

Part I: Privacy Shield Replaces Safe Harbor

Many US businesses are familiar with the EU-US Privacy Shield and its analogue, the Switzerland-US Privacy Shield (jointly referred to as the "Shield"), which was agreed to by the U.S. Department of Commerce (DOC), the European Commission (Commission), and Switzerland. The Shield is the latest mechanism now validly in force to enable US entities to be in compliance with personal data transfer requirements in Europe. It is based upon EU Member State implementation of the 1995 European Data Protection Directive (95/46/EC), which is, and will continue to be, the law in effect for the next half-year until the 1995 Directive is superseded by the GDPR (see below).

The Shield was developed to replace the formerly utilized Safe Harbor (Commission Decision 2000/520/EC of 26 July 2000), which was invalidated by the European Court of Justice (ECJ) in the case of Maximilian Schrems v. Supervisory Authority. Consequently, as of October 31, 2016, the DOC stopped accepting all US-EU Safe Harbor certifications. The Safe Harbor was held by the ECJ to be insufficiently safe to protect the personal data of EU citizens and residents, thus paving the way for the Shield.

On August 1, 2016 after the Commission had deemed the Shield adequate to enable data transfers under current EU law, the DOC began accepting certifications from U.S. companies to join the program (81 FR 47752; July 22, 2016). The Shield provides for self-certification from US companies that have privacy policies and practices in place that comply with the provisions of the Shield. Although over 2400 entities have already self-certified, there is a real possibility that legal challenges to the efficacy of the Shield will eventually prevail. This could result in a holding that the Shield, like the Safe Harbor before it, does not adequately protect the personal data of EU citizens.

Actually, the Shield is only one of several mechanisms enabling US and European companies to be in compliance with data protection requirements when transferring personal data from the European Union (and/or Switzerland) to the United States. For example, other approved means for cross-border data transfers are Standard Contractual Clauses ("SCC") and Binding Corporate Rules ("BCR"), although the latter method is much more difficult to adopt and generally has much less flexibility, and consequently is

likely not to be the mechanism of choice for most US companies. Most organizations have been opting for the more flexible and more simply implemented Shield or SCCs.

The Shield provides for a joint annual review, the first of which took place in September 2017. The joint press release following the review was not particularly substantive: "The United States and the European Union share an interest in the Framework's success and remain committed to continued collaboration to ensure it functions as intended."

Self-certification for the Shield by US organizations is easy to do online. However, self-certifying and then not adhering to the Shield's compliance requirements would likely be costly in the long term. Under the Federal Trade Commission (FTC) Act, US entities' failures to implement business practices that comply with the Shield can be deemed as deceptive trade practices and the US can enforce adherence through administrative orders or court orders. Violations of those orders can result in civil penalties of up to $40,000 per day or per violation. In a similar way, failure of implementation by air carriers or ticket agents could be held in violation of 49 USC 41712 and also result in fines and penalties in similar amounts. Persistent failure to comply can result in an organization's removal from the Shield and thus also its inability to transact further business with EU Member States and Switzerland.

The Shield principles include the "Notice Principle," which requires informing individuals about the organization's participation in the Privacy Shield and providing a link to, or the web address for, the Privacy Shield List. Organizations must identify the types of personal data collected, committing that the Privacy Shield requirements will be followed relative thereto, and they must disclose to the data subject the purposes for which they collect and use that person's personal data. It also requires listing information regarding how to contact the organization for any inquiries or complaints, including how to contact any relevant establishment in the EU and/or Switzerland that can respond to such inquiries or complaints. Organizations must: (i) identify the type or identity of third parties to which it discloses personal data, and the purposes for which it does so; (ii) clearly state the right of individuals to access their personal data, and how individuals can limit the use and disclosure of their personal data; and (iii) identify the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual. Finally, under the Notice Principle, the organization must state that it is required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and it must explain its liability in cases of onward transfers to third parties.

Importantly, the notice must be provided in clear and conspicuous language when individuals are first asked to provide personal data to the organization, or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization, or when it discloses it for the first time to a third party.

Between the United States and Europe, proper data treatment is essential. Since the European data protection requirements are arguably more stringent than data protection requirements in the United States, noncompliance with them could mean not doing business in or with Europe. The penalties and consequences are too heavy. But, getting the Commission to agree with the United States on a mechanism for US corporate compliance with European data protection laws has not been easy, nor has it been noncontroversial. Many Europeans remain skeptical about the ultimate efficacy of the Shield,

particularly in the wake of the Edward Snowden affair, which showed, inter alia, that the US Government was violating the spirit of the Safe Harbor with the cooperation of a number of US technology companies.

Despite this, many on both sides of the Atlantic have been optimistic that the Shield constitutes an effective solution to the limitations of the Safe Harbor; others, however, continue to doubt that it will solve the concerns of privacy groups. In any event, it's arguably the best game in town for the moment to legally transfer personal data from the European Union to the United States. A cautionary note to US companies providing self-certification: it is not enough to certify that you are in compliance. Your compliance programs must be designed not only in accordance with the Shield provisions but they must also be implemented and properly monitored to avoid serious legal consequences.

Accordingly, US businesses and other entities processing personal data should be adopting policies that take into consideration the provisions of the EU General Data Protection Regulation that will come into force in May, 2018, and they should anticipate that the Shield could eventually succumb to legal challenges a la Safe Harbor. Indeed, challenges are already afoot.

Part II: EU General Data Protection Regulation 2016/679 (GDPR) Replaces EU Data Protection Directive 95/46/EC

During the same time frame that the Shield was being designed and implemented, the EU was engaged in a project to update and replace its existing data protection provisions (the ones for which the Shield is intended to provide compliance). The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize privacy and data security laws across Europe and to reshape the way organizations across the region approach data protection. Because it is a Regulation, and not a Directive, it will be directly applicable in all EU Member States in May, 2018. By comparison, a Directive would instead only require that each state enact its own national law that satisfies the directive's requirements.

Article 1 of the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data (and it) protects fundamental rights and freedoms of natural person and in particular their right to the protection of personal data..."

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing of personal data takes place therein, and it could apply to the processing of personal data in the European Union by a controller or processor not established in the European Union.

After four years of planning and work, the GDPR was approved by the EU Parliament on April 14, 2016, and therefore entered into force 20 days after its publication in the EU Official Journal; it will be directly applicable in all members states two years after this date. Its official starting date, therefore, is May 25, 2018. Organizations not in compliance at that date may be subject to heavy fines.

This leads to a practical query: Would organizations participating in the Shield be considered to be in compliance with the GDPR? With regard to processing personal data transferred under and in accordance with the Shield, it would appear that they would be in compliance; however, any processing of EU personal data outside of the Shield does not necessarily mean that there is GDPR compliance. And, as stated

earlier, the mere fact of self-certifying, but not meeting the underlying criteria as set forth above, would expose organizations nominally protected under the Shield, to serious consequences in terms of their ability to conduct operations with Europe, not to mention liability to pay fines of up to twenty million Euros or 4% of their worldwide turnover, whichever is greater.

Again, it should also be kept in mind that potential challenges to the Shield now under way in Europe could invalidate it, in which case, US entities must have robust and actively monitored procedures and policies in place that meet all the requirements of the GDPR. Mere reliance on self-certification will not be sufficient going forward. It is a wise, if not essential, practice for clients to be prepared for the GDPR in all respects, even if already "protected" by the Shield.

Therefore, organizations must have in place procedures and policies that will be adequate to satisfy the inevitable, future challenges by persons claiming they are inadequately protected by the Shield.

***

Aaron Schildhaus is Counsel to Scharf, Banks & Marmor, PC, a Chicago law firm, specializing in corporate litigation and transactions. His practice is focused on US – EU data protection and privacy compliance, FCPA compliance and due diligence, and international transactions involving the US, Europe, Africa, India, the Middle East and Latin America, representing NGO's and large and small corporations in the US and abroad. He is past Chair of the ABA Section of International Law and has spoken frequently internationally, and written numerous articles, on data protection in Europe and on a wide variety of other business related legal topics**.**