HUNTON& WILLIAMS

Lawyer Insights

August 5, 2016

EU-US Privacy Shield: A Path Forward

Risks, Benefits and the Future of the Agreement

by Lisa J. Sotto and Christopher D. Hydak

Published in Corporate Compliance Insights

The European Commission formally adopted the EU-US Privacy Shield in July 2016 after more than two years of negotiation with US regulators. On August 1, 2016, the Department of Commerce began accepting certification applications from US companies that have agreed to comply with the Shield's seven principles. Similar to its predecessor regime known as the Safe Harbor, which was invalidated by the European Court of Justice in October 2015, the Privacy Shield is a data transfer mechanism that allows companies in the US to receive personal data from the European Union in compliance with EU cross-border data transfer restrictions.

After the Safe Harbor was invalidated and before the Privacy Shield was unveiled, companies in the US that previously had relied on the Safe Harbor for their trans-Atlantic data flows had little choice but to implement alternative mechanisms for transferring personal data from the EU to the US. The two primary alternative data transfer mechanisms, known as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), each have a number of drawbacks, as discussed below. In addition to these transfer mechanisms, there are several exceptions to the EU transfer restrictions that permit transfers of personal data from the EU to the US, such as transfers that are made pursuant to data subject consent and those that are necessary to serve the legitimate interests of the exporting company or the data recipient. But these exceptions are not intended to allow the systematic and continuous transfers of data required by today's businesses, and many European data protection authorities view these exceptions skeptically and interpret them narrowly. Now that the Privacy Shield has been formally adopted, many US companies are left wondering whether to certify to the Privacy Shield or stick with the alternate data transfer frameworks they put in place before the Privacy Shield was rolled out.

Benefits of the Privacy Shield

A number of the most onerous aspects of SCCs and BCRs are not repeated in the Privacy Shield framework. SCCs, for example, present both procedural and substantive complexities. From a procedural perspective, in several EU Member States, companies must obtain regulatory approval to use SCCs as a legitimate data transfer mechanism. In other Member States, although regulatory approval is not required, SCCs nevertheless must be submitted to the relevant EU Member States' data protection authorities. In addition, SCCs are inflexible — the provisions of the European Commission-approved clauses may not be altered in any way. If the provisions are changed, the contract is no longer considered a valid mechanism by which to legally transfer data outside of the EU. From a substantive perspective, SCCs fare no better. For example, SCCs require data importers outside of the EU to allow the relevant EU data

exporters to audit the importers' data processing facilities. This is a difficult ask for large US service providers such as cloud storage providers that have thousands of clients. BCRs, while a highly effective mechanism for data transfers once implemented, typically take more than a year to put into place and require the expenditure of significant monetary and human resources. As a result, fewer than 100 companies worldwide have implemented BCRs as their data transfer mechanism.

The Privacy Shield is much more flexible than SCCs and does not require the significant investment necessary to implement BCRs. To certify to the Privacy Shield, a business in the US must agree to abide by the seven principles that comprise the Shield. These principles, which include requirements for the certifying organization to provide EU individuals with notice about the business's data-handling practices and choices with respect to certain uses and disclosures of personal data, resemble the corresponding EU data protection principles. Typically, a company considering certifying to the Privacy Shield would spend several months assessing its data management processes, conducting a gap analysis and developing the internal policies and procedures necessary to comply with the Privacy Shield. Once the underlying work has been completed and the company has certified its compliance with the Privacy Shield principles, the organization may receive personal data in the US from an unlimited number of EU data exporters, including the company's affiliated entities in the EU. Although certifying to the Privacy Shield requires a commitment of time and resources, the investment necessary to certify (and undertake the required annual re-certification) is far less significant than that required to implement BCRs.

Risks Associated with the Privacy Shield

The biggest risk associated with the Privacy Shield, and the risk that leaves many US companies hesitant to certify, is that the Privacy Shield could suffer the same fate as the Safe Harbor. Like the Safe Harbor, the Privacy Shield is likely to undergo a legal challenge that could render the framework invalid as a legal mechanism by which to transfer personal data from the EU to the US. Certain EU privacy advocates have already indicated that they plan to bring a legal challenge because they believe the Privacy Shield's protections do not sufficiently safeguard the rights and freedoms of EU data subjects.

There is also a risk that the Privacy Shield could be found to provide inadequate protection under the EU General Data Protection Regulation, which is due to come into force in May 2018. The Privacy Shield's existing adequacy decision is based on the current EU data protection regime under the EU Data Protection Directive, and that regime will be replaced in full in less than two years.

Although the Privacy Shield's fate is uncertain, its odds of survival are strong. The drafters of the Privacy Shield sought to address each issue identified by the European Court of Justice in its decision invalidating the Safe Harbor. While not bulletproof, the Privacy Shield likely is sufficiently carefully crafted to be able to withstand a legal challenge. Importantly, the Privacy Shield will be reviewed by EU and US government representatives on an annual basis, providing an opportunity for the relevant regulators on both sides of the Atlantic to tweak the framework, remediate vulnerabilities and clarify ambiguities.

The Verdict

The Privacy Shield is likely to be a popular choice for US companies to legitimize their receipt of personal data from the EU. Several large US technology companies have already signaled their intention to certify to the Privacy Shield, and many other US-based organizations undoubtedly will follow suit. For those companies that receive in the US a significant amount of personal data from the EU, the Privacy Shield is an attractive choice of data transfer mechanisms. Given the flexibility offered by the Privacy Shield and the protections it provides to EU individuals, there is reason to be optimistic about the Privacy Shield's future.

EU-US Privacy Shield: A Path Forward
by Lisa J. Sotto and Christopher D. Hydak
Corporate Compliance Insights | August 5, 2016

Lisa J. Sotto is a partner and chair of the global privacy and cybersecurity practice at Hunton & Williams in New York. She assists clients in identifying, evaluating and managing privacy and information security law risks. She may be reached at (212) 309-1223 or lsotto@hunton.com. Christopher D. Hydak focuses his practice on privacy, data security and information management issues. He may be reached at (212) 309-1012 or chydak@hunton.com.