HUNTON& WILLIAMS

Lawyer Insights

July 19, 2016

The EU-US Privacy Shield: A How-To Guide

by Lisa J. Sotto and Christopher D. Hydak

Published in Law360

The EU safe harbor framework, unveiled in 2000, allowed certified U.S. companies to receive personal data of EU residents in compliance with EU cross-border data transfer rules. The safe harbor served as a popular data transfer mechanism for U.S. companies — more than 4,000 businesses had certified to the safe harbor, including many service providers whose ability to legally transfer data to the U.S. allowed thousands of other businesses to comply with EU data transfer restrictions. Despite its popularity, however, 15 years after the safe harbor was rolled out by European and U.S. regulators, it was declared invalid by the stroke of a pen held by the Court of Justice of the European Union. The CJEU's opinion was largely motivated by the belief that the safe harbor, and U.S. law in general, did not adequately protect the fundamental rights and freedoms of EU individuals whose information was transferred to the U.S. pursuant to the safe harbor because there were not sufficient restrictions on the U.S. government's ability to grab that data once in the hands of U.S. companies.

Four months after the CJEU invalidated the safe harbor, in February 2016, the European Commission released the EU-U.S. Privacy Shield. The Privacy Shield was designed to replace the safe harbor and cure the deficiencies identified by the CJEU. Following its issuance, a number of EU-based government bodies (including the Article 29 Working Party, European Parliament and European Data Protection Supervisor) and consumer privacy advocates criticized aspects of the shield. In an effort to address the concerns, EU and U.S. regulators renegotiated and revised a few sections of the Privacy Shield text, including those involving onward transfers and data retention. A revised version of the Privacy Shield was formally adopted on July 12, 2016, as a successor to the now-defunct safe harbor.

The U.S. Department of Commerce has indicated that it will begin accepting certifications from U.S. companies on Aug. 1, 2016. Commerce worked quickly to release in July 2016 a guide to self-certification and FAQs.

Purpose of the Privacy Shield

EU data protection law generally prohibits the transfer of personal data outside of the EU unless the transfer (1) is to a jurisdiction that is deemed by the EC to provide an "adequate" level of protection for EU personal data, (2) falls within one of the few exceptions, or (3) is made in accordance with one of a small number of legal data transfer mechanisms. There are few "adequate" jurisdictions globally and the U.S. is not one of them. The exceptions, which include consent of the relevant individual, are ill-suited to routine and systematic business transfers. With respect to legal mechanisms for transferring EU personal data, the Privacy Shield is one of the few methods available, along with standard contractual clauses and binding corporate rules, by which personal data can be legally transferred from the EU to the U.S. Unlike

This article presents the views of the authors and do not necessarily reflect those of Hunton & Williams LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.

standard contractual clauses and binding corporate rules, the Privacy Shield is available only to companies in the U.S. and applies only to data transfers from the EU to the U.S.

Privacy Shield Requirements

To use the Privacy Shield as a data transfer mechanism, similar to the safe harbor, U.S. companies must commit to comply with seven principles governing the handling of personal data received in the U.S. via the shield. The seven principles that comprise the Privacy Shield are comparable to those of the safe harbor. The names of the principles have changed slightly, more detail has been added to certain of the principles, and a few new items have been included. Generally, however, companies that previously were certified to the safe harbor will be able to transition to the Privacy Shield without an extensive review or alteration of their processes for handling personal data received from the EU.

The Privacy Shield principles, along with brief descriptions of each principle, are as follows:

1. Notice — Organizations must inform relevant EU data subjects of thirteen enumerated data handling practices, such as the types of personal data the entity collects and how it uses the data.

2. Choice — Companies must offer individuals the opportunity to opt out if their personal data is to be (a) disclosed to a third party (except agents) or (b) used for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized.

3. Accountability for Onward Transfer — Businesses must enter into written contracts with third parties to whom they transfer personal data received from the EU; those contracts must contain specific protections for the data.

4. Security — Organizations must take reasonable and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. Data Integrity and Purpose Limitation — Entities must (a) limit personal information to that which is relevant for the purposes of the relevant processing, (b) take reasonable steps to ensure personal data is reliable for its intended use and is accurate, complete and current, and (c) retain personal data only for as long as it serves a purpose of the relevant processing.

6. Access — Companies must provide relevant EU individuals with access to the personal data the organization holds about them, as well as the ability to correct, amend or delete that information where it is inaccurate or has been processed in violation of the Privacy Shield.

7. Recourse, Enforcement and Liability — Businesses must implement robust mechanisms for assuring compliance with the Privacy Shield, including an independent recourse mechanism for complaints and procedures for verifying the privacy representations made to individuals.

The seven principles of the Privacy Shield are complemented by 16 supplemental principles that provide more detail regarding specific data transfer issues, such as the processing of human resources information or sensitive data. Because the principles are designed to reflect the protections for personal data and rights granted to data subjects under EU law, companies with operations in the EU should be familiar with the substance of the shield's requirements.

© 2016 Hunton & Williams LLP

Why Certify?

Like the safe harbor, the Privacy Shield is expected to be popular among U.S. companies seeking to receive personal data from the EU. The Privacy Shield is more flexible, more convenient and less costly for companies to implement than other available data transfer mechanisms. For example, standard contractual clauses often are viewed as an administrative nightmare. All relevant legal entities may need to sign the clauses (including all data exporters and importers), certain EU member states require data exporters to submit the clauses, and other EU member states mandate regulatory approval of the clauses before transfers may commence. In addition, standard contractual clauses contain provisions that many data importers find onerous, such as the requirement to submit data processing facilities to audits by the data exporter and to obtain the exporter's consent to provide subcontractors with access to personal data. Binding corporate rules require the approval of EU data protection authorities and generally involve a lengthy and costly process. A large multinational organization could expect to spend well over a year and expend significant resources (both monetary and otherwise) to implement binding corporate rules.

Organizations that will derive the most benefit from the availability of the Privacy Shield are those that route the majority of their EU-originating personal data from the EU to the U.S. For example, a U.S.-based company whose Texas headquarters serves as the global hub for the organization's data will find the Privacy Shield particularly useful. If the company certifies to the shield, it can legally transfer EU personal data to the U.S. The company also will be allowed to transfer the personal data to third-party recipients who have signed an "onward transfer" agreement prepared by the company. Organizations that transfer their EU data directly to countries other than the U.S. generally will not be able to take advantage of the Privacy Shield.

To induce companies to certify early, the Privacy Shield contains a narrow nine-month grace period for organizations that certify within the first two months of the Privacy Shield's effective date. Businesses that certify during this two-month window will have a nine-month transition period to bring their existing contracts with onward transfer recipients into compliance with the Privacy Shield. Companies that certify more than two months after the effective date must have all of their shield-related onward transfer agreements in place on the date of certification.

Enforcement

Certifying to the Privacy Shield imposes a legal commitment to comply with the seven principles of the shield. The Federal Trade Commission and the U.S. Department of Transportation are authorized to enforce against violations of the Privacy Shield. Companies that certify and fail to comply with the shield are subject to enforcement by these regulators. The FTC, which is the principal U.S. enforcement agency with respect to the shield, brought nearly 40 enforcement actions for violations of the safe harbor. The FTC is expected to be even more active in enforcing compliance with the Privacy Shield. A company that violates the requirements of the shield likely would enter into a consent order imposing stringent data handling obligations for 20 years.

Future of the Privacy Shield

The EC's decision validating the Privacy Shield is based on Directive 95/46/EC, which is the current data protection regime in the EU. As has been widely publicized, Directive 95/46/EC is set to expire on May 25, 2018, when its successor framework, the General Data Protection Regulation will take effect. The GDPR will fundamentally transform the EU data protection regime. While deemed to provide adequate protection to personal data under Directive 95/46/EC, the Privacy Shield may not be found adequate under the GDPR.

© 2016 Hunton & Williams LLP

A more likely risk, as evidenced by the demise of the safe harbor, is a CJEU decision to overturn the Privacy Shield's adequacy decision in response to a legal challenge. While such a challenge appears inevitable, and the CJEU's response to such a challenge is difficult to predict, the Privacy Shield is expected to fare better than the safe harbor because the shield's provisions were specifically drafted to address the inadequacies identified by the CJEU in the safe harbor.

There is reason to be optimistic about the future of the Privacy Shield. Unlike the safe harbor, the shield will undergo a joint annual review by EU and U.S. authorities. Should material concerns arise, they can be addressed through ongoing revisions to the text. The safe harbor framework was static and became stale over time. By its nature, the annual review process will ensure that the shield remains current.

Given the changes in technology and world events since 2000, an overhaul of the safe harbor was inevitable, particularly in light of the Snowden revelations and the upcoming revamp of the EU data protection regime. The Privacy Shield was the result of three years of negotiation by EU and U.S. authorities. The final product shows the significant efforts on the part of the negotiating team to address all outstanding concerns so as to leave little room for questions regarding the adequacy of the protections provided by the shield to EU residents' personal data. The text of the shield was carefully crafted to satisfy EU concerns about its predecessor regime's lack of rigor in key areas, such as the ability of U.S. law enforcement to access EU personal data, redress for EU residents, and the onward transfer of data to third parties. The European Commission's approval of the shield is a win for global commerce. The enhanced protections provided to EU data are a win for EU privacy rights. All in all, the new EU-U.S. Privacy Shield is a coup for all stakeholders.

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.

© 2016 Hunton & Williams LLP