Hogan Lovells
CHRONICLE of DATA PROTECTION
PRIVACY & INFORMATION SECURITY NEWS & TRENDS

Posted on July 12th, 2016 By Julie Brill, Bret Cohen, Eduardo Ustaran, Jonathan Stoel and Harriet Pearson

# Privacy Shield Receives Final Approval from European Commission—Some Initial Practical Advice

On 12 July 2016, the European Commission issued its much awaited "adequacy decision" concerning the Privacy Shield framework for the transfer of personal data from the EU to the U.S. This adequacy decision is based on the latest version of the Privacy Shield, which was further negotiated and revised following the Article 29 Working Party's April 2016 concerns with the terms of the original Privacy Shield framework.

Many of our clients have questions about Privacy Shield—what it is, when it will be available for use, and how it differs from other data transfer mechanisms, among others. We have prepared a blog post to answer these questions about the updated version of Privacy Shield and its implications for companies engaging in trans-Atlantic data flows.

**What is Privacy Shield?**

In 2000, the United States Department of Commerce and the European Commission devised the "Safe Harbor" privacy framework to protect the rights of European citizens as their data traveled across the Atlantic. American companies that agreed to self-certify to the seven Safe Harbor principles were allowed to collect and use data originating from the EU, and store such data on U.S. servers.

By October of last year, some 4,500 U.S. companies, large and small, were relying on Safe Harbor to transfer employee and consumer data from the EU to the U.S. That month, the Court of Justice of the European Union (CJEU) invalidated Safe Harbor as a data transfer mechanism in the case *Schrems v. Data Protection Commissioner*. The CJEU held that, in approving Safe Harbor in 2000, the European Commission did not appropriately consider whether it provided EU personal data with the right level of protection. The Department of Commerce and European Commission redoubled existing efforts to produce a successor framework to Safe Harbor that would address the concerns of the CJEU and European stakeholders.

The result of these efforts is Privacy Shield. Similar to Safe Harbor, companies may rely on the Privacy Shield framework for data transfer by self-certifying their compliance with seven Privacy Shield principles. However, Privacy Shield provides greater protections to EU citizens than Safe Harbor—both substantively and procedurally—and thus will likely result in a greater level of data protection for EU personal data.

**Who can rely on Privacy Shield?**

As with Safe Harbor, U.S. businesses subject to the jurisdiction of the Federal Trade Commission or Department of Transportation can rely on the Privacy Shield framework. Thus, the scope of Privacy Shield covers most U.S. for-profit businesses, but excludes a number of banks, financial services companies, and other businesses that are not subject to the jurisdiction of those regulatory agencies.

**How and when can a company participate in Privacy Shield?**

Companies will be able to participate in Privacy Shield by filing an online registration with the Department of Commerce starting on 1 August 2016.

**What are the seven principles with which companies must comply under Privacy Shield?**

The seven principles with which Privacy Shield companies must comply are similar to the principles under Safe Harbor. However, each of them has been strengthened in important ways, especially the principle of recourse, enforcement and liability.

The seven principles are:

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement, and Liability

**What steps should companies take before they self-certify to the Privacy Shield framework?**

Privacy Shield requires companies that self-certify compliance with the Privacy Shield principles to take certain steps to demonstrate that they can comply, including:

- Conducting an internal compliance assessment to determine the company's ability to comply with the principles with respect to information that will be covered by the certification. To the extent there are any gaps in its ability to comply, the company should adopt internal controls, policies, and procedures to come into compliance.

- Registering with a third-party arbitration provider to handle any complaints from EU individuals about the handling of their information that the company is unable to fully resolve, and pay any registration fees.

- Adopting a Privacy Shield notice that contains thirteen specified details about the company's privacy practices, and publish the notice online.

**What are the benefits of participating in Privacy Shield?**

Companies that participate in Privacy Shield will be able to offer to their EU business partners and affiliates a means to lawfully transfer personal data to the United States. Under EU law, these organizations cannot lawfully transfer personal data to entities in the United States without taking steps to assure that the U.S. entity will be

able to adequately protect the information. The Privacy Shield will help these EU organizations comply with this legal obligation.

Since Safe Harbor was invalidated by the CJEU, many companies have been using Standard Contractual Clauses to legitimize transfers of EU personal data to the United States. The Privacy Shield can replace these Standard Contractual Clauses and some of the other complex contractual arrangements that are allowed as Safe Harbor alternatives under EU law.

In addition to receiving personal data from EU entities, Privacy Shield also will enable U.S. companies to more easily receive EU personal information from other Privacy Shield participants—so joining will make sense for a number of U.S. service providers. In addition, joining Privacy Shield is likely to give a general level of comfort to various EU (and non-EU) government regulators, officials, and business partners that a company takes seriously the privacy of personal data.

**What are the risks?**

Companies that certify compliance with the Privacy Shield principles and fail to comply subject to enforcement by the Federal Trade Commission or Department of Transportation for engaging in unfair or deceptive trade practices. Therefore, it is important for companies to assess their compliance with the Privacy Shield principles before certifying.

Because of the significant publicity around EU-to-U.S. data flows and the invalidation of Safe Harbor for perceived deficiencies, Privacy Shield will be subject to significant scrutiny after its adoption. European privacy regulators and advocates likely will "kick the tires" on the new arrangement with respect to companies that they perceive are not complying.

Privacy Shield also enhances redress procedures for EU individuals, so participating companies may see an uptick of complaints and the use of those redress procedures.

**What should companies with a Safe Harbor certification do?**

U.S. companies that previously certified to Safe Harbor should consider certifying to Privacy Shield. However, companies should not assume that their compliance with the Safe Harbor principles means that they also will be in compliance with the Privacy Shield principles, as there are a number of new substantive obligations. Therefore, it is crucial for these companies to confirm that they are able to comply with all of the Privacy Shield principles.

The Department of Commerce will phase out the Safe Harbor program (which it had left operative pending the Privacy Shield negotiations), so U.S. entities that are still certified to the Safe Harbor program should phase out that participation, including by removing public references to their participation in Safe Harbor. However, if a company retains personal data it obtained under Safe Harbor, it must continue to abide by the Safe Harbor principles until the data is deleted or de-identified.

**Will Privacy Shield be challenged like Safe Harbor?**

From the public statements made by a number of privacy activists—including Max Schrems himself—it is very likely that Privacy Shield will be put to the test in the CJEU. Ongoing concerns about government surveillance have been cited as the main reasons for a potential legal challenge.

If so, it will take several months and possibly years before the CJEU makes a final decision on the adequacy of Privacy Shield as a data transfer mechanism. However, it is important to note that the negotiations between the European Commission and the U.S. Department of Commerce have been specifically aimed at addressing the issues that affected Safe Harbor, so it is by no means certain that the CJEU would rule against Privacy Shield. A detailed legal assessment of the initial draft of the Privacy Shield against the CJEU adequacy criteria carried out by Hogan Lovells in March 2016 argued that the Privacy Shield substantially met the criteria laid out by the CJEU.

*More information on Privacy Shield and practical next steps will be provided at an upcoming Hogan Lovells webinar. To receive notifications of and additional details regarding upcoming Hogan Lovells Privacy and Cybersecurity events, please subscribe to our blog.*

---

Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004 | USA
Phone: +1 202 637 5600
Fax: +1 202 637 5910

Hogan Lovells International LLP
Atlantic House
Holborn Viaduct
London EC1A 2FG
United Kingdom
Phone: +44 20 7296 2000
Fax: +44 20 7296 2001