SHEARMAN & STERLING LLP

CLIENT PUBLICATION

PRIVACY AND DATA PROTECTION | JULY 13, 2016

European Commission Adopts the EU-US Privacy Shield

If your organization works with personal data across national borders, you may have felt a tremor as the global data privacy landscape shifted once again. On July 12, 2016, the European Commission formally approved the EU-US Privacy Shield, finding that the Privacy Shield Framework provides adequate protections for European Union (EU) residents to permit transfer of their personal data from the EU to the US. The Privacy Shield Framework also provides much-needed clarity for businesses through a unified set of principles and obligations. US-based businesses will be able to use the Privacy Shield as soon as August, with the US Department of Commerce accepting self-certifications beginning August 1, 2016.

EU and US authorities had been working since 2014 to strengthen protections of EU residents' personal data in transfers to the US, and those efforts intensified in the wake of the October 2015 decision of the Court of Justice of the European Union (CJEU), *Schrems v. Data Protection Commissioner*. In *Schrems*, the CJEU invalidated the previous framework, the US-EU Safe Harbor, on the grounds that it failed to adequately protect EU residents' personal data. The *Schrems* decision created significant uncertainty in EU to US data flows.

The Privacy Shield Framework seeks to replace Safe Harbor by providing an efficient solution for EU to US data flows. By self-certifying to the Department of Commerce annually and adhering to the Privacy Shield Principles, businesses may transfer EU residents' personal data to the US in compliance with EU privacy laws.

From Harbor to Shield—What's Different?

The Privacy Shield was designed to address issues raised by the CJEU in the *Schrems* decision. Although the Privacy Shield implements certain principles, similar to Safe Harbor, it differs in several respects. The Privacy Shield Framework establishes seven Privacy Shield Principles and sixteen Supplemental Principles, resulting in stronger obligations on US companies handling personal data, defined means of redress available for EU individuals, enforcement commitments from US agencies, safeguards on US government access, and continuing monitoring of the program itself.

Stronger obligations in handling data. Similar to Safe Harbor, the Privacy Shield works as a self-certification system, but under the Privacy Shield Framework, the Department of Commerce will verify self-certification materials and afterwards require updates and conduct reviews to confirm that participants follow the policies and materials included in the self-certification. There are additional transparency requirements, and participants must regularly verify compliance, either through internal processes or by engaging a third party. Participants must also follow more stringent obligations in the onward transfer of EU personal data to third parties.

Redress for EU individuals. Under the Privacy Shield Framework, participants must make specific redress mechanisms available to EU individuals. EU individuals may bring complaints directly to Privacy Shield participants. The participant will have 45 days to respond and must have an independent dispute resolution process available at

no cost. An EU individual may also submit their complaint to a data protection authority (DPA) in the EU. The DPA will bring the complaint to the Department of Commerce, which must use best efforts to facilitate a resolution and respond to the DPA within 90 days. EU individuals may also pursue any available causes of action in US courts, and may invoke binding arbitration for complaints not resolved through other means.

Enforcement. In the US, the Federal Trade Commission (FTC) and Department of Transportation (DOT) have committed to "vigorous enforcement" of the Privacy Shield Framework, using any investigatory and civil enforcement means available. The FTC will prioritize referrals of possible violations from EU DPAs, the Department of Commerce, privacy self-regulatory organizations, and EU individuals, in addition to investigating potential violations on its own initiative. Potential sanctions for noncompliance include monetary penalties, consent orders with submission to ongoing independent privacy assessments, injunctions, and suspension or removal from Privacy Shield participation, which could require destruction of personal data transferred under the Privacy Shield. Enforcement actions and any resulting sanctions will likely be publicized.

Safeguards to US government access. US agencies have assured the European Commission that US access to EU personal data for law enforcement and national security purposes will be targeted and limited, and subject to authorization and oversight. In addition, the US State Department will implement a Privacy Shield Ombudsperson mechanism, identifying an individual outside of the US intelligence apparatus who will address and resolve complaints relating to US national security. These are important developments; US government access to personal data was one of the key reasons cited in *Schrems* to invalidate Safe Harbor.

Monitoring. The European Commission, FTC, Department of Commerce, and other EU and US authorities, as appropriate, will hold annual meetings to review and evaluate the Privacy Shield Framework, including implementation and enforcement efforts.

Key Takeaways

- Self-certification to the Department of Commerce is a legally enforceable commitment, and from the time that an organization submits its self-certification materials, it must comply with the Privacy Shield Principles and Framework.
- A Privacy Shield participant must be responsive and have mechanisms in place to handle and resolve complaints from EU individuals. To respond effectively, a participant will need specific, granular understanding of its data flows and use of personal data within its organization, as well as relevant documentation to support its response.
- The FTC has committed to vigorously enforce the Privacy Shield Framework, including in cooperation with EU DPAs and based on private referrals. Since EU DPAs and individual privacy advocates have historically taken more active approaches to enforcing privacy and data protection laws, it remains to be seen how such cooperation will work in practice or how other parties may seek to leverage the FTC's commitment.

Lifting the Shield—Participation in the Privacy Shield Framework

Now that the European Commission has formally adopted the Privacy Shield, it will be notified to EU member states and immediately enter into force. In the US, the Privacy Shield Framework will be published in the Federal

Register, and the Department of Commerce will be responsible for its operation, accepting self-certifications beginning August 1, 2016.

There is no obligation to participate in the Privacy Shield Framework, and as discussed, there are significant requirements on participants. US businesses should consider whether it makes sense to participate in the Privacy Shield Framework, and if it does, thoughtfully implement a plan and policies to meet its requirements. The self-certification to the Department of Commerce is a commitment to comply with the framework's requirements, which is enforceable under US law.

For businesses that decide to participate in the Privacy Shield, they must conform to all Privacy Shield Principles and related guidance. For example, a participant must:

a. be eligible to participate, meaning that the organization is subject to the jurisdiction of the FTC or DOT;

b. ensure that its privacy policy complies with the disclosure and substantive requirements of the Privacy Shield Framework, and that the privacy policy is fully implemented and publicly available;

c. set up and identify the organization's recourse mechanisms;

d. conform onward transfers of personal data to third parties to the Privacy Shield Framework; and

e. submit the required self-certification materials to the Department of Commerce, then maintain compliance and self-recertify annually for as long as the organization is a participant.

The Department of Commerce will review and verify the self-certification materials. If the self-certification is complete, the Department of Commerce will place the participant and its self-certification materials on the Privacy Shield List, and the participant will receive the benefits of the Privacy Shield starting on that date.

For businesses that decide not to use the Privacy Shield, there are other means to permit data flows from the EU to US, but each has its own drawbacks. Personal data may still be transferred under the Standard Contractual Clauses, but doubts have been raised as to the Clauses' validity and vulnerability to actions similar to *Schrems*. The Data Protection Commissioner of Ireland announced in May 2016 that she will seek legal review of the Clauses by the Irish High Court and CJEU. Companies may also consider binding corporate rules (BCRs), which tend to be appropriate only for large multinational companies and are not often used in practice. The approval process for BCRs is currently lengthy and expensive, and that process is expected to change with the EU's planned adoption of the General Data Protection Regulation (GDPR). Consent of the data subject may also support international transfers, but it is not workable in many circumstances.

Key Takeaways

- The Privacy Shield is substantively different from Safe Harbor, and businesses should not assume that self-certifying to the Privacy Shield will be trivial, or that they can carry over Safe Harbor certification. Businesses considering participation should review and understand all requirements under the Privacy Shield Framework to determine whether participation is suitable for them.
- All compliance efforts must be documented in order to respond to complaints or enforcement investigations.

- To conform onward data transfers to third parties, businesses will often need to revisit the terms of such data transfers. (Because this impacts existing contractual relationships, there are certain allowances for entities that self-certify within the first two months of the program. Any other participants must be compliant prior to self-certification.)

Future of the Privacy Shield

Given the upheavals in data transfer laws over the past year, it may be unsurprising that the Privacy Shield has already been criticized for failing to sufficiently protect the privacy rights of EU individuals—though it is generally seen as an improvement over Safe Harbor. Max Schrems, the privacy advocate who challenged Safe Harbor, views the Privacy Shield as an improvement but claims that it will be just as vulnerable to legal challenge as Safe Harbor.

Some uncertainty around the Privacy Shield appears inevitable, but among current options, US-based businesses may reasonably view the Privacy Shield as the preferred means to allow EU to US data transfers. Companies considering participation might also keep in mind that investing in Privacy Shield Framework compliance will mean investing in improved handling and protection of personal data. The Privacy Shield requirements are likely to become features of future cross-border data transfer regimes. In an environment where privacy and data protection issues are more visible, where US states and agencies are increasingly involved in cybersecurity, and where data security breaches have ever more impact on the bottom line, these may be worthwhile investments to make.

Key Takeaways

- Despite the inevitable criticisms and lingering uncertainty, the Privacy Shield Framework may reasonably be viewed as the most viable current option for EU to US data transfers.
- In the current environment, addressing and strengthening privacy and data protection practices to satisfy the Privacy Shield Framework will likely have benefits beyond Privacy Shield compliance.

SHEARMAN & STERLING LLP

CLIENT PUBLICATION

CONTACTS

Jeewon Kim Serrato
Washington, DC
+1.202.508.8032
jeewon.serrato@shearman.com

Richard C. Hsu
Menlo Park
+1.650.838.3774
richard.hsu@shearman.com

Barney Reynolds
London
+44.20.7655.5528
barney.reynolds@shearman.com

Andreas Löhdefink
Frankfurt
+49.69.9711.1622
andreas.loehdefink@shearman.com

Thomas Donegan
London
+44.20.7655.5566
thomas.donegan@shearman.com

Mathias Stöcker
Frankfurt
+49.69.9711.1619
mathias.stoecker@shearman.com

Marc Elzweig
Menlo Park
+1.650.838.3815
marc.elzweig@shearman.com

599 LEXINGTON AVENUE | NEW YORK | NY | 10022-6069