Overview

On February 29, 2016, the European Commission and the US Department of Commerce (DOC) jointly released the text of the proposed new “Privacy Shield” agreement allowing the transfer of data from the European Union to the United States in compliance with the EU Data Protection Directive. The Privacy Shield will not take effect until the European Commission issues an “adequacy decision” confirming that the Privacy Shield meets the requirements of the Data Protection Directive.

The Privacy Shield agreement is a large and complex document – well over 100 dense pages, much of it descriptions and commitments by the US government regarding US privacy protections. In this initial look at the agreement, we focus on three important issues:

- Requirements for companies that wish to join the Privacy Shield, and how they differ from those of the former Safe Harbor
- New enforcement and dispute resolution mechanisms
- The way forward to adoption of the agreement

Joining the Privacy Shield: Similar to Safe Harbor with Differences in the Details

The good news for companies planning to use the Privacy Shield is that it is structurally very similar to the Safe Harbor. Like the Safe Harbor, the Privacy Shield provides for self-certification with the US DOC that a company’s privacy policies for EU data follow specified requirements. The process covers all companies that are regulated by the US Federal Trade Commission (FTC) and Department of Transportation. As for the Safe Harbor, the major sectors not covered (which could be added in the future with cooperation between the EU and relevant US regulators) are financial services (regulated by the US Securities and Exchange Commission) and telecommunications (regulated by the US Federal Communications Commission).

Furthermore, the general areas of privacy compliance required by the Privacy Shield are the same as those in the Safe Harbor. The high-level compliance areas covered by the Privacy Shield Framework Principles (the Principles) are nearly identical to those under the Safe Harbor:

- Notice
- Choice
- Accountability for Onward Transfer (Onward Transfer under the Safe Harbor)
- Security
- Data Integrity and Purpose Limitation (Data Integrity under the Safe Harbor)
- Access
- Recourse, Enforcement and Liability (Enforcement under the Safe Harbor)
However, there are some significant changes in the details of the Principles from the Safe Harbor to the Privacy Shield. For example, there is significant additional detail in the Notice principle (which will require many companies to add additional detail to their privacy policies) and an explicit requirement of contracts for onward transfer of data. The Principles also include fairly lengthy Supplemental Principles, replacing and augmenting the Frequently Asked Questions under the Safe Harbor. And enforcement under the Privacy Shield will become more complex and stricter, as discussed in the next section.

Significantly Enhanced Enforcement and Dispute Resolution

Enhanced enforcement was a significant focus in the negotiations of the Privacy Shield, as emphasized in the European Commission communication this week releasing the text of the agreement. Three areas of enforcement deserve particular attention: (1) mechanisms for private enforcement, (2) monitoring and enforcement by the US authorities, and (3) recourse mechanisms for uses of data for US national security purposes.

Mechanisms for Private Enforcement. As under the Safe Harbor, the Principles require a certifying company (a) to make available an “independent recourse mechanism” for disputes (with increased specificity on how such a mechanism must function), (b) to cooperate with EU data protection authorities, or some combination of (a) and (b). In addition, the Principles require Privacy Shield participants to arbitrate “residual claims” that have not been resolved after being pursued with the participating company, the independent recourse mechanism, and the US DOC; and the Principles provide that the Department of Commerce will establish a fund to pay the costs of such arbitration through annual fees to Privacy Shield participants (which will be based in part on company size).

US Monitoring and Enforcement. The US DOC and FTC have committed to enhance monitoring of compliance and enforcement under the Privacy Shield. This will include increased scrutiny of Privacy Shield self-certifications by the US DOC, and stricter increased enforcement by both agencies against false certifications (which was the primary focus of FTC enforcement under the Safe Harbor) and non-compliance with the Principles.

National Security Recourse. A primary concern of the European Court of Justice in overturning the Safe Harbor in the Schrems case was the access of US authorities to data, largely as revealed by Edward Snowden. National security remains an explicit carve-out from Privacy Shield requirements. However, the US government in the Privacy Shield has (a) made extensive representations regarding US law in this area (including under PPD-28 adopted by President Obama in reaction to the Snowden revelations), (b) agreed to the new arbitration mechanism discussed above, and (c) agreed to appoint an Ombudsperson responsible for dealing with EU concerns regarding national security monitoring (the position will initially be held by Undersecretary of State Catherine Novelli).

Way Forward to Adoption of Privacy Shield

In order for the Privacy Shield to take effect, it must be approved through a detailed “adequacy decision” by the European Commission, which has been released in draft. The next step in the process will be consideration of the draft adequacy decision by the Article 29 Working Party of EU data protection authorities, which has issued a statement that it intends to adopt an opinion on the Privacy Shield at its meeting on April 12-13. Objections to the Privacy Shield will certainly be raised in that process, and it remains to be seen whether such objections will be sufficient to require negotiations between EU and US authorities on changes to the agreement.

In summary, good progress has been made towards adoption of a workable Privacy Shield (albeit one that is materially more complex than the Safe Harbor), but it is too soon to tell whether and when this new agreement will be available to support data transfers from the European Union to the United States.