Privacy and Information Governance


By Mary Ellen Callahan and Sabrina N. Guenther

Today, the European Commission (the Commission) published the final text of the long-awaited U.S.-EU Privacy Shield (Privacy Shield), along with new annexes and fact sheets. On July 8, 2016, the Article 31 Committee, composed of representatives of each EU member state, approved the Privacy Shield and essentially marked the culmination of the process to clarify the state of play regarding transatlantic personal data flows after the European Court of Justice (ECJ) invalidated a previous transatlantic agreement, the U.S.-EU Safe Harbor Program (Safe Harbor). The Privacy Shield will officially replace Safe Harbor on August 1, 2016.

The Privacy Shield Debate: February to July 2016

The final version of the Privacy Shield comes after several months of debate over the proposed February 2016 version of the agreement. The February draft came under fire when the Article 29 Working Party, the collection of EU data protection authorities (DPAs), opined in April 2016 that Privacy Shield would confuse data subjects and failed to provide sufficient protections for Europeans’ personal data. While the Article 29 Working Party’s opinion was non-binding, it led members of the Article 31 Committee to express concerns about Privacy Shield’s adequacy prior to the Committee’s binding vote.

To address the Article 31 Committee’s concerns (influenced by the DPAs), the European Commission and the U.S. Department of Commerce recently agreed to clarify certain Privacy Shield Principles (Principles) in the agreement itself and in other associated materials.

The Delta: Key Changes for the Final Privacy Shield

The final Privacy Shield agreement retains the bulk of the February 2016 text and amends particular portions in response to four primary issues raised by the Article 29 Working Party and the Article 31 Committee. As before, a U.S. company that participates in the Privacy Shield via annual self-certification and handles personal data related to European data subjects agrees both (1) to comply with European DPAs’ decisions regarding that data, and (2) to submit to oversight of its compliance with Privacy Shield obligations by the Department of Commerce and the Federal Trade Commission (FTC). Moreover, the core Principles enumerated in the earlier version remain the same: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement, and Liability. The Principles are set forth in Privacy Shield Annex II.

The changes to the final Privacy Shield text focus on four areas:

Clarifying Contractual Obligations Surrounding Onward Data Transfers. The final Privacy Shield text
provides more detail regarding contractual requirements for third parties that receive onward transfers of personal data from a Privacy Shield organization. As before, the Privacy Shield organization remains responsible for compliance with the Principles when it transfers personal data about an EU resident to a third party. The final version of Privacy Shield specifies two important points. First, it clarifies that the Privacy Shield obligations apply even if the third party that receives personal data about EU residents is located outside the U.S. and the EU. Second, the final version of Privacy Shield stipulates that any onward transfer and downstream use must either be compatible with the original purpose of collection or specifically authorized by the affected data subject. In addition, the final text provides that the third party recipient of a personal data from a Privacy Shield organization must both notify the Privacy Shield organization if it can no longer meet its obligations under the Principles and take appropriate steps to redress any unauthorized processing.

Limiting Personal Data Retention. The final Privacy Shield text also clarified the data retention requirements in the Data Integrity and Purpose Limitation Principle. Under the final text, a Privacy Shield organization may retain personal information only for as long as it is “relevant for the purpose of the processing, reliable for its intended use, accurate, complete, and current.” A Privacy Shield organization must take particular care if personal data is retained in an identifiable form (as opposed to aggregated or de-identified). Privacy Shield does not articulate a specific time period for personal data retention, instead applying a purpose-driven standard.

Refining Complaint Mechanisms for Data Subjects. As in the February 2016 draft, Europeans who believe that a Privacy Shield organization has improperly handled their personal data under the Principles can pursue several avenues of redress. The available methods for redress, complaint handling, and enforcement under the final Privacy Shield remain largely the same as those in the earlier text. As before, these mechanisms operate in addition to Department of Commerce and FTC enforcement of Privacy Shield Principles. Minor changes in the final text include:

- Clarifying the role of the Ombudsman at the Department of State. As provided in the February 2016 draft, DPAs can refer a request or complaint regarding access to personal data by U.S. intelligence agencies to a new Ombudsman established in the U.S. Department of State. The final Privacy Shield stresses the Ombudsman’s objectivity and independence, although the final text provides no concrete new responsibilities or authorities for the Ombudsman.

- Specifying that a DPA who receives a complaint from an individual citizen may—but is not obligated to—refer the matter to either the Department of Commerce or the FTC.

Clarifying National Security Parameters. Though less relevant for commercial entities, the final Privacy Shield text further explains the nature of “bulk data collection” in the U.S. and the EU and also describes the operation and governance of the U.S. national security and intelligence community. This language attempts to distinguish current U.S. national security practices from the “mass, indiscriminate surveillance” that the ECJ cited in its decision to invalidate Safe Harbor.

Next Procedural Steps

The next steps for the Privacy Shield are fairly minor procedural matters. Today, the EU member states will receive notification of the Commission’s approval of Privacy Shield (adequacy decision), after which the decision officially enters into force. The Article 29 Working Party will vote on the revised document in late July, though it cannot veto the agreement. The final document also must be translated into the 23 official languages of the EU before it takes effect; the translations have been in process using the February text, therefore this step should not delay implementation, given the limited textual changes from February to July, which appear in only a handful of sections. The European Commission and the Department of Commerce project that the Privacy Shield will take effect on August 1, 2016.

Once the Privacy Shield takes effect, its requirements will apply immediately to any organization that self-
certifies its compliance to the Privacy Shield with the U.S. Department of Commerce. The Privacy Shield includes, however, a limited nine-month grace period for organizations who certify within two months of the effective date – by October 1, 2016, based on the projected August 1 effective date – to bring their existing commercial relationships with third parties into compliance with the Accountability for Onward Transfer Principle.

**Takeaways**

Though it might be tempting to seek shelter under the Privacy Shield as soon as possible, each company should engage in an individualized assessment to consider whether doing so makes sense given that company’s particular data flows and current data protection practices.

The likelihood of a future challenge to the Privacy Shield and ongoing uncertainty regarding the United Kingdom’s status in the EU also merit careful consideration. In light of these uncertainties, some companies may wish rely on other valid transfer mechanisms for EU personal data.

Alternative methods for transferring EU personal data to the United States include model contract clauses, ad-hoc data transfer agreements, and binding corporate rules. Some of these mechanisms – including model contracts – may be subject to further approval requirements from the relevant EU member state(s). Further, the Irish DPA recently referred to the Irish High Court a challenge to the adequacy of model contracts to transfer personal data to the U.S. Before settling on one or more of these methods, companies should analyze the extent of their global data flows, in what manner and at what volume any third parties or vendors will process personal data from the EU, and how a potential challenge to Privacy Shield in the ECJ would affect their long-term data protection strategy, particularly as they prepare for implementation of the EU General Data Protection Regulation in May 2018.

*Thanks to summer associate Alicia Solow-Niederman for her assistance on this Alert.*

**Contact Us**

**Mary Ellen Callahan, Partner, Jenner & Block**

Phone: 202 639-6064    Email: mecallahan@jenner.com    Download V-Card

Mary Ellen Callahan chairs Jenner & Block’s Privacy and Information Governance Practice and provides privacy and data security counseling to a broad range of clients, including some of the most visited online properties. She served as Chief Privacy Officer of the US Department of Homeland Security from 2009 to 2012 and was named a Cybersecurity & Privacy Trailblazer by the *National Law Journal* in 2015.

**Sabrina N. Guenther, Associate, Jenner & Block**

Phone: 312 840-7299    Email: sguenther@jenner.com    Download V-Card

Sabrina N. Guenther is an associate in the firm’s Privacy and Information Governance Practice. She has experience counseling clients with respect to privacy and cybersecurity risks on both a national and international scale.