## Transatlantic Agreement Translated: *Language of U.S. - EU Privacy Shield Released*

By Mary Ellen Callahan, Heidi Wachs, Sabrina Guenther, and Emily Bruemmer

Today the European Commission released the text of the proposed U.S.-EU Privacy Shield framework for transatlantic data flows (the "Privacy Shield"). The Commission also released a draft adequacy decision, which would approve the Privacy Shield as providing an adequate level of data protection for transfers of personal data from the EU to the U.S. in accordance with the EU Data Protection Directive, 95/46/EC, and details about the U.S.-EU Umbrella Agreement, which addresses data protection standards for transatlantic data transfers for law enforcement purposes. The Privacy Shield text and draft adequacy decision still face further review and approval processes in the EU before companies may consider and rely on the Privacy Shield as a valid transatlantic data transfer mechanism.

If approved, the Privacy Shield would replace the long-standing U.S.-EU Safe Harbor Agreement, which had been in place since 2000 and was recently held to be invalid by the European Court of Justice ("CJEU") in a decision on October 6, 2015.

### The Privacy Shield Principles

The Privacy Shield Principles include: Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability, set forth in Annex 2. Although the top line privacy Principles are similar to Safe Harbor Privacy Principles, the Privacy Shield Principles are much more detailed and granular. They also include a number of "Supplemental Principles," which offer more detailed requirements for specific circumstances, such as the transfer of sensitive data, the self-certification process, and the role of the European Data Protection Authorities ("DPAs"), etc.

These Principles enhance the Principles from the former Safe Harbor program in several important respects. Some highlights include:

> **Increased Regulatory Oversight**. The U.S. Department of Commerce ("DOC") will monitor companies' compliance with their public commitments, and the Federal Trade Commission will enforce U.S. companies' public commitments to abide by the data protection obligations in the new framework. The DOC has committed to conduct ongoing reviews and monitoring, including *ex officio* compliance and assessment reviews, of companies' self-certification to and compliance with the Privacy Shield Principles. These ongoing monitoring activities include searching for and identifying any false claims of participation, and taking corrective actions, including reporting to the appropriate enforcement authorities, when such behavior is discovered. The DOC also committed to establishing a dedicated liaison and standardized complaint referral process between it and the DPAs to receive and help resolve complaints of non-compliance with the Privacy Shield.

In connection with its implementation of the Privacy Shield, DOC will maintain a Privacy Shield website that provides resources to EU individuals, EU businesses, and U.S. businesses. The DOC's website will also provide a link to a list of Privacy Shield-related FTC enforcement actions, and lists of U.S. organizations currently self-certified to the Privacy Shield principles. The DOC may remove organizations from the Privacy Shield list if the organization fails to complete its annual re-certification, voluntarily withdraws, or if DOC determines it has persistently failed to comply with the Privacy Shield Principles.

U.S. companies that handle personal data related to European employees must commit to comply with decisions regarding such data by European DPAs in addition to the DOC's and FTC's oversight.

**Multiple Complaint Mechanisms for Data Subjects**. European citizens who believe that their personal data has not been handled according to the Privacy Shield will have several options with respect to redress. **First**, they are encouraged – but not required – to file a complaint with the Privacy Shield organization, which must respond to the complaint within 45 days. **Second**, data subjects will have access to several "independent recourse mechanisms," which must provide readily available recourse free of charge to data subjects. Independent recourse mechanisms must also publicly post information on the Privacy Shield Principles and the Privacy Shield-related services they provide, as specified in the Principles, and must publish annual reports with aggregated statistics regarding their dispute resolution services. **Third**, data subjects may raise complaints with their member state's DPA, which will forward the matter to the Department of Commerce. If the request or complaint involves access to personal data by the U.S. intelligence community, the DPAs may refer those issues to a new Ombudsman to be established under the U.S. Department of State. **Finally**, after pursuing redress through the first three methods above, data subjects may proceed to arbitration against the Privacy Shield organization.

These individual redress mechanisms will operate in addition to the Federal Trade Commission's enforcement of the Privacy Shield Principles. The FTC will investigate potential unfair or deceptive trade practices in connection with the Privacy Shield, as it did in connection with the Safe Harbor program.

**Increased Accountability for Onward Transfers**. Companies certified under the Privacy Shield must comply with additional requirements to ensure that any EU personal data remains protected if and when the companies transfer the data to third parties. Essentially, Privacy Shield companies must ensure that, in cases of onward transfers to third parties, they employ contractual agreements requiring ongoing protections equivalent to the Privacy Shield Principles. The precise requirements for these agreements differ depending on whether the third-party recipient acts as a "controller" or an "agent." By contrast, a multi-national company participating in the Privacy Shield may transfer personal data among controllers within its organization subject to its compliance and control programs (as opposed to contracts), so long as those programs ensure the continuity of protection of personal information under the Privacy Shield Principles.

In all of these cases of onward transfer, the Privacy Shield organization remains responsible for compliance with Privacy Shield Principles.

**Law Enforcement and National Security**. For the first time as part of an international negotiation, the United States Department of Justice and Office of the Director of National Intelligence made public statements (included in Annex 6 and Annex 7 of the draft adequacy decision) about how law enforcement and national security agencies handle personal information on non-U.S. persons. The statements included thorough discussion of relevant U.S. law (including Executive Orders and Presidential Policy Directives). However, the nuances of these statements may be lost on ordinary EU (or even U.S.) readers, given the level of detail and specialized jargon used in the statements. Notably, the statements did not acknowledge that Constitutional protections are often weakened outside of the United States, particularly for non-U.S. persons. In addition, they failed to acknowledge that Executive Orders and Presidential Policy Directives can be changed by each President, which is particularly relevant given the upcoming Presidential election in the U.S.

In sum, the law enforcement and national security statements were well-intended, but, in light of the specialized legal terminology and an audience unfamiliar with U.S. legal systems, they likely do not meet the goal of providing transparency and comfort to EU readers.

**Next Procedural Steps**

The Article 29 Working Party, along with representatives from the EU member states (as required by Article 31 (2) of the Directive), will now begin reviewing the text of the Privacy Shield and other documents to provide a decision on whether the Privacy Shield meets the adequacy standards for data transfer. The EU College of Commissioners may, after receiving input from these various parties, finally determine whether to approve the Privacy Shield.

While approval of the Article 29 Working Party is not required for the Privacy Shield to become valid, practically speaking, the stability and credibility of the Privacy Shield as a transatlantic data transfer mechanism – and therefore its success – may suffer without the group's approval.

Further, even if the EU Commission determines that the Privacy Shield provides adequate protections for the transfer of personal data to the U.S., the Privacy Shield may face further legal challenges in EU courts. In its October 6, 2015 decision invalidating Safe Harbor, the CJEU expressed a number of concerns regarding transfers of personal data to the U.S. Some EU constituents, including the Safe Harbor challenger, Maximilian Schrems, have expressed doubt regarding whether the Privacy Shield satisfies the CJEU's concerns. If the Privacy Shield is challenged, the CJEU could invalidate the Privacy Shield as an adequate transatlantic transfer mechanism, effectively overruling the EU Commission (just as it did in the Safe Harbor decision).

**Takeaways**

While regulatory review of the Privacy Shield continues, companies can now begin analyzing the Privacy Shield principles in light of their own data flows and data protection practices.

Companies should weigh the measures they would need to take to comply with the Privacy Shield principles against other valid transfer mechanisms for EU personal data. (Model clauses, ad-hoc data transfer agreements, and binding corporate rules remain valid methods for transferring EU personal data to the U.S., though each of these methods may be subject to member state-specific approval requirements.) Companies also should take into account, however, the risk that the CJEU could invalidate the Privacy Shield, even if it is approved by the Article 29 Working Party, member state representatives, and EU College of Commissioners.

If the Privacy Shield is approved, companies can participate through annual self-certifications to the Privacy Shield Principles. The self-certification process for the Privacy Shield would be similar to the certification process required under the now-defunct Safe Harbor program, although the standards associated with the Privacy Shield Principles are much more robust.

For these reasons, companies should weigh carefully the Privacy Shield Principles and the enhanced obligations on developing complaint mechanisms and limiting onward transfer before commencing review and self-certification with the Privacy Shield.

*Thanks to visiting attorney Dr. Stefan Alich of Taylor Wessing for his contributions to this article.*