WILMERHALE

EU-US Privacy Shield Framework Principles Released

MARCH 1, 2016

Racing to meet the Article 29 Working Party's end of February deadline for more documentation on the proposed EU-US Privacy Shield, the European Commission and US Department of Commerce released a collection of documents on Monday, February 29, summarizing actions taken on both sides of the Atlantic to implement the new Privacy Shield framework. This framework is designed to replace the "Safe Harbor" regime that was invalidated by the European Court of Justice in October 2015. Of significant note, the Department of Commerce (Commerce) released a detailed set of Privacy Shield Framework Principles while the European Commission released a draft adequacy decision on the Privacy Shield. This draft decision explains how the new framework provides "an adequate level of protection" under EU law for personal data transferred to self-certified US companies. The decision will need to be formally adopted and published in the Official Journal of the EU before the Privacy Shield can become an effective mechanism for data transfers.

To assist with that process, Commerce has produced a package of materials to support the Commission's adequacy finding. These materials discuss safeguards and legal limits imposed on both the intelligence community and the Department of Justice for access to personal data. They also include Privacy Shield commitments by a number of different agencies, including Commerce, the State Department, the Department of Transportation, and the Federal Trade Commission (FTC).

The new arrangement will increase obligations on participating US companies and will require stronger monitoring and enforcement efforts by US regulators, including the FTC. To take advantage of the Privacy Shield as a basis for transferring personal data from the EU to the United States, US companies will need to:

- self-certify adherence to the new framework's Principles (and re-certify annually thereafter);
- verify their public Privacy Shield commitments through either a self-assessment or an outside compliance review;
- agree to be responsive to inquiries for information about their Privacy Shield compliance; and
- respond to any individual complaints within forty-five days. The Privacy Shield framework further envisions several additional layers of consumer redress for EU individuals.

The Principles also impose new transparency obligations and require new contractual

commitments for onward data transfers.

In a letter to the European Commission, the FTC has committed to prioritizing referrals from both EU Member States and self-regulatory bodies regarding potential Privacy Shield noncompliance.[1] The FTC will create a standardized referral process and provide additional guidance, and it intends to work more closely with European data protection authorities (DPAs), including through information-sharing and investigative assistance.[2] Privacy Shield violations also will be explored in the course of the FTC's existing privacy and data security investigations.

Department of Commerce's Privacy Shield Framework Principles

The Department of Commerce also will be heavily involved in the administration and supervision of the new program. Compared to its administration of the Safe Harbor, Commerce has pledged to double the number of staff responsible for supervising the Privacy Shield, and it has further committed to conducting official reviews and assessments of the program.[3] Most significantly, Commerce will actively search for and address misrepresentations of companies' participation, referring matters to the FTC for enforcement action where appropriate.[4]

The Privacy Shield provides additional detail with respect to the seven high-level principles of the Safe Harbor. Where the Safe Harbor used the headlines of (1) notice, (2) choice, (3) onward transfer, (4) security, (5) data integrity, (6) access, and (7) enforcement, the Privacy Shield details similar but expanded Principles of (1) notice, (2) choice, (3) accountability for onward transfer, (4) security, (5) data integrity and purpose limitation, (6) access, and (7) recourse, enforcement, and liability.[5] Some of the material in these expanded Privacy Shield Framework Principles formalizes information that had been included in the Safe Harbor Frequently Asked Questions, but several new obligations imposed by these Principles include:

- Expanded Notice Obligations: In addition to disclosures informing individuals of their access rights to personal data, explaining that personal data may be disclosed in response to lawful requests from public authorities, and detailing the company's liability for onward transfers of personal data to third parties, Privacy Shield companies are required to provide information and direct links to Commerce's website and its forthcoming "Privacy Shield List." Links to more information about an appropriate, cost-free alternative dispute resolution provider also must be provided.
- New Contract Requirements and Liability for Onward Transfers: Onward transfers of personal data now are permitted only (1) for limited and specified purposes, (2) on the basis of a contract, and (3) where that contract provides the same level of protection for the data as the Privacy Shield would offer. Should any compliance problems arise in the sub-processing chain, Privacy Shield companies are assumed to be responsible and liable for any damage. Recognizing that this could be a difficult transition, the framework grants companies that join within its first two months nine months to bring existing commercial onward transfer relationships into compliance.
- Additional Access Rights: The Privacy Shield grants EU-style access rights to individuals regarding their personal data. Under the framework, individuals have the right to obtain confirmation as to whether a company holds personal data relating to them and to have

that information communicated to them. No justification is required, and companies may not charge excessive fees for such access. Access rights may be denied or limited only in exceptional circumstances.

- Cooperation with Regulators: Commerce will actively monitor compliance with the Privacy Shield. Participating companies must promptly respond to inquiries and requests about their compliance with the framework. Commerce also has committed to conducting compliance reviews of companies, which could include detailed questionnaires, and will carry out reviews in response to specific complaints, where companies fail to provide satisfactory responses to its inquiries, or where credible evidence exists that a company is not complying with the framework. If a company leaves the Privacy Shield, it must remove all public statements implying continued participation in the framework.
- Redress Mechanisms: The Privacy Shield envisions several different redress possibilities. First, as a baseline, individuals must be permitted to file complaints directly with Privacy Shield companies. Second, individuals may bring complaints directly to DPAs, who will work with Commerce and the FTC to resolve any unresolved complaints or issues. In both instances, companies must provide the individual with a reply within forty-five days that assesses the merits of the complaint and explains how the company intends to rectify any shortfalls in compliance. Third, Privacy Shield companies must offer an alternative dispute resolution provider free of charge. Finally, as a mechanism of "last resort," individuals may invoke binding arbitration by a "Privacy Shield Panel" selected from arbitrators designated by Commerce and the European Commission.

The Privacy Shield resembles the Safe Harbor's principles around choice and security:

- Choice Principle: The Privacy Shield requires companies to allow individuals to "opt out" of having their personal data (1) disclosed to third parties, other than to agents and service providers, or (2) used for "materially different" purposes than those for which it was collected. This resembles the Safe Harbor's requirement that individuals have the ability to choose whether their personal information is disclosed to third parties or used for incompatible purposes.
- Security Principle: The Privacy Shield continues the Safe Harbor's requirement that participating companies implement "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the personal data being created, maintained, used, or otherwise disseminated.

Persistent failure to comply with these obligations will permit the Commerce to remove a company from its "Privacy Shield List." Refusing to comply with orders by "any privacy self-regulatory, independent dispute resolution or government body, including a DPA," is considered a persistent failure to comply, and could warrant removal from the Privacy Shield. In the event a Privacy Shield company becomes subject to an FTC order for non-compliance with the framework, the consent order will contain self-reporting provisions and the company will be required to make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with any confidentiality requirements.

Additionally, the new Privacy Shield Framework Principles include a set of supplemental principles that provide further detail about the how to implement access rights, self-certify, and subsequently verify that self-certification. The supplemental principles also set out requirements and practices around certain specific types of information:

- The framework continues to recognize a general exception for public communication of "journalistic material." Personal data gathered for publication or broadcast, whether used or not, is not subject to the requirements of the Privacy Shield framework.
- Key-coded research data that is transferred to the United States is not considered a transfer of personal data that would be subject to the Privacy Shield framework.
- As under the Safe Harbor, companies that transfer human resources data must agree to cooperate and comply with European DPAs with respect to that data. Additionally, companies must provide Commerce with a copy of their human resources privacy policy and provide information as to where that policy is made available to employees.

Annual Joint Review Mechanism

An important feature of the Privacy Shield framework is that it may evolve over time. The European Commission and Commerce will conduct annual joint reviews of the operation of the Privacy Shield program. According to the European Commission, this effort will "not be a formalistic exercise without consequences" and will allow all parties to "regularly monitor the functioning of all aspects of the Privacy Shield."

The review will involve national intelligence experts from the United States and representatives from European DPAs. Further, the Commission will hold an annual privacy summit with non-governmental organizations and other stakeholders to discuss developments in US privacy law and its potential impact on individuals in the European Union. These activities, as well as industry-led transparency reports, will inform public reports by the European Commission to the European Parliament and the Council on the future status of the Privacy Shield. As the Commission explains, "US companies and authorities have to breathe life into the framework and continuously sustain it by living up to their commitments."

What's Next?

US companies have largely embraced the new framework. However, it likely will take some time before the European Commission's draft adequacy decision for the Privacy Shield framework is formally approved and published in the Official Journal of the EU, and the Principles do not go into effect until then.

Much work remains on both sides of the Atlantic before the Privacy Shield can be implemented. According to the European Commission, both the EU DPAs (through the Article 29 Working Party) and a committee of European Member State representatives will be consulted while US officials work to implement the necessary public-facing tools and enforcement resources to ensure the success of the framework. Only then will a final decision on the Privacy Shield be made by the European Commission.

[1] Letter from Edith Ramirez, FTC Chairwoman, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 5 (Feb. 23, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/927423/160229ftc_privacyshieldletter.pdf.

[2] *Id.* at 6. *See also* US SAFE WEB Act, 15 U.S.C. § 46(j)(3) (providing the FTC with a number of tools to enhance cooperation with foreign law enforcement authorities).

[3]Letter from Stefan M. Selig, Under Secretary for International Trade, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission, at 6 (Feb. 23, 2016), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-1_en.pdf.

[4] *Id*. at 5.

[5] US Dept of Commerce, EU-US Privacy Shield Framework Principles 4-7 (Feb. 29, 2016), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Prof. Dr. Hans-Georg Kamann

PARTNER

Vice Chair, Antitrust and Competition Practice

hans-georg.kamann@wilmerhale.com

+49 69 27 10 78 204

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP