HWG CLIENT ADVISORY – EU-U.S. PRIVACY SHIELD SELF-CERTIFICATION PROCESS NOW OPEN

William Leahy & Mary Huang*

On August 1, 2016, the U.S. Department of Commerce began accepting self-certification applications from U.S.-based companies to join the EU-U.S. Privacy Shield Framework, a new mechanism for U.S. companies to comply with EU data protection requirements when importing personal data from the European Economic Area.

Formally adopted by the European Commission on July 12, the Privacy Shield is the culmination of more than two years of negotiations between the EU and the United States. It replaces the EU-U.S. Safe Harbor, a fifteen-year-old transatlantic data transfer framework invalidated by Europe's highest court in October 2015. Compared to its predecessor, the Privacy Shield commits participants to a more robust set of principles aimed at strengthening data protection and enforcement mechanisms.

In the weeks since the Privacy Shield's launch, the Department of Commerce has received a large number of applications and anticipates more will follow. The Department of Commerce also began listing certified companies on the program website (here).

Although participation in the Privacy Shield is voluntary, compliance is compulsory. Once a company self-certifies and publicly declares its commitment to comply, this commitment is enforceable under U.S. law. The following provides a brief overview of the Privacy Shield's principles along with the self-certification process.

Privacy Shield Principles. Participants must commit to seven primary principles and 16 supplemental principles:

1. Notice: A company must inform individuals about its participation in the Privacy Shield, its commitment to the Principles, the types of personal data collected, and the purposes for which it collects them, including the type or identity of third parties to which such data may be disclosed. Additionally, a company must inform individuals of their right to access their own personal data, ability to limit or tailor the types of data collected, and ability to invoke binding arbitration or utilize the independent dispute resolution system designed to address complaints and provide recourse free of charge. At minimum, notice must be provided before the company discloses the personal data for the first time to a third party or uses the data for anything beyond the original purpose for collection or processing.

2. Choice: Companies must obtain individuals' affirmative consent (opt-in) before transmitting any sensitive information to a third party or for a use materially

different from the original purpose for collection. Sensitive information includes medical conditions, race or ethnicity, political opinions, religious beliefs, and trade union membership. For non-sensitive information, companies must provide individuals with the ability to choose whether their personal information can be disclosed to a third party or be used for a materially different purpose (opt-out).

3. Accountability for Onward Transfer: In order to transfer data to third parties, companies must adhere to the Notice and Choice principles. They also must enter into a contract with the third party to ensure the transferred data may only be used for limited and specified purposes consistent with the consent provided by the individual. The contract must bind the third party to provide the same level of privacy protection under the Privacy Shield Principles and notify the company if the third party can no longer meet this obligation. Upon notice, the company must take reasonable steps to stop and remediate any unauthorized data processing.

4. Security: Companies creating, maintaining, using and/or disseminating personal information must take reasonable steps to prevent loss, misuse, unauthorized access, disclosure, alteration or destruction.

5. Data Integrity and Purpose Limitation: Companies must limit collection of personal information to information relevant for processing purposes (e.g. customer relations, compliance, auditing, security and fraud prevention, or other purposes consistent with reasonable expectations given the context of collection). A company cannot process information in a way that is incompatible with the purpose for which it has been collected or otherwise authorized by the individual. And companies can only retain personally identifiable information for as long as it serves such processing purposes.

6. Access: Companies must grant individuals access to the information collected about themselves and the opportunity to correct or delete inaccurate information, unless providing access would violate other individuals' rights or impose a burden disproportionate to the privacy risks.

7. Recourse, Enforcement and Liability: Companies must provide recourse mechanisms to address individual complaints alleging non-compliance with Privacy Shield Principles. At minimum, these must include readily available independent recourse mechanisms for investigation of complaints – free of charge to the individual, follow-up procedures for verifying the company's attestations and assertions about their privacy practices, and obligations to remedy problems arising from non-compliance. As a last-resort option, individuals can invoke binding arbitration. Companies must follow the terms of the Privacy Shield's arbitral model.

The Supplementary Privacy Principles outline specific requirements for categories such as sensitive information, journalistic exceptions, liabilities for Internet Service Providers, performing due diligence and conducting audits, the role of EU Data Protection Authorities, and self-certification and compliance verification procedures.

Navigating the Self-Certification Process. To join the Privacy Shield, companies must self-certify annually to the Department of Commerce via the program website (here). The site sets out a five-point plan for companies to ensure their self-certifications can be accepted:

1. Check eligibility. Any U.S. organization subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) may participate. Most banks and telecommunications carriers, for example, fall outside of FTC jurisdiction and are thus ineligible.
2. Develop or update privacy policies to meet all Privacy Shield Principles. Make sure the policies are clear-cut and publicly available.
3. Identify the independent recourse mechanism your company will use to settle disputes. This information must also be included in the privacy policy, and the recourse mechanism must be in place prior to self-certification.
4. Identify procedures in place for verifying compliance with the Privacy Shield Principles. This may be accomplished through a first-party or third-party assessment program.
5. Designate a Privacy Shield contact within the company who will be able to handle questions, complaints, access requests, and other issues. Companies must respond to complaints within 45 days.

Companies that submit their applications within the first two months of the August 1 start date can take an additional nine months from the submission date to ensure their contracts for onward transfer with third parties are in compliance with Privacy Shield Principles. All other applicants must ensure such contracts are in compliance at the time of submission.

As for program fees, the Department of Commerce charges an annual tiered processing fee ranging from $250 for companies with revenue under $5 million to $3,250 for those with revenue over $5 billion. Additionally, participants have to pay to join an arbitration service or to cover the costs of data protection authorities handling complaints. The amount for annual contributions to cover arbitral costs has yet to be set by Commerce and the European Commission, but it will be finalized within six months of July 12, 2016 (date of the Privacy Shield's adoption).

* * * * *

For more information regarding the EU-U.S. Privacy Shield Framework and self-certification process, please contact William Leahy at (202) 730-1358 or wleahy@hwglaw.com. Alternatively, you should contact the HWG lawyer with whom you regularly work.

*Summer law clerk. Not admitted to practice in any state.