WILMERHALE

Privacy Shield Moves Forward, Company Certifications to Begin August 1

JULY 12, 2016

The European Commission formally adopted the EU-US Privacy Shield on Tuesday, ending months of legal uncertainty with a new framework for governing transatlantic data transfers after the Privacy Safe Harbor framework was invalidated in 2015. According to the Commission, Privacy Shield shifts from being a system based on self-regulation to "an oversight system that is more responsive as well as proactive" via stronger efforts by the US Department of Commerce, the US Federal Trade Commission and European Data Protection Authorities. The US Department of Commerce is now encouraging companies to review the framework, and it will begin accepting voluntary certifications beginning on August 1.

In addition to an array of new safeguards placed on US mass surveillance on personal data transferred to the US, the final text of the Privacy Shield also imposes stronger data protection obligations on participating US companies that receive personal data from the European Union. Specific features include:

- First, the US Department of Commerce is now responsible for conducting regular reviews of participating companies and ensuring that companies follow the rules.
- Second, there are now tightened conditions for "onward transfers" by participating companies to third parties. Third party recipients must be contractually required to provide the "same level of protection" as required of the Privacy Shield participant, and to inform that company if it can no longer ensure an appropriate level of data protection.
- Third, the principle of data retention has been made more explicit—participating companies may keep personal data only as long as it serves the purpose for which the data was collected.
- Further, any EU data subject may complain if they feel their rights have been violated; this right extends to any individual whose data originates from the EU and not just EU nationals.

The US Department of Commerce's Privacy Shield Team will conduct industry briefings to provide information about the certification process, and has released a "Guide to Self-Certification" to help companies as they prepare to certify.

As with the defunct Safe Harbor framework, the decision to join the Privacy Shield remains entirely voluntary, but once a company publicly commits to the framework through self-certification, that commitment will be legally enforceable. The US Department of Commerce encourages companies to consider the following steps to meet the requirements for self-certification:

1. **Confirm your organization's eligibility to participate in Privacy Shield:** As with Safe Harbor, only companies that are subject to the jurisdiction of the US Federal Trade Commission or Department of Commerce may participate.
2. **Identify your organization's independent recourse mechanism:** Privacy Shield companies must provide a mechanism for investigating privacy-related complaints at no cost to EU data subjects. This mechanism must be in place prior to self-certification. Companies may either use a private sector dispute resolution program or may agree to cooperate and comply with EU Data Protection Authorities.
3. **Develop a Privacy Shield-compliant privacy policy statement:** A company's public privacy policy must satisfy the Privacy Shield's principles before a company may self-certify. Further, a privacy policy must expressly refer to the company's compliance with Privacy Shield, identify the selected an independent recourse mechanism, and be publicly available.
4. **Ensure your organization's verification mechanism is in place:** Companies must put in place procedures—either via self-assessment or through third-party assessment programs—to verify their continuing compliance with Privacy Shield requirements.
5. **Designate a contact within your organization regarding Privacy Shield:** Companies must designate a point of contact for handling questions, complaints, access requests and other issues arising under the Privacy Shield and EU data protection law. Importantly, companies must respond to individuals within 45 days of receiving a complaint or request.

Relevant Documents:

- **EC's Press Release**
- **The EC's Adequacy Decision**
- **Updated Privacy Shield Annex Documents**
- **Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards**
- **EU-US Privacy Shield: Frequently Asked Questions**
- **Factsheet**

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770