July 18, 2016

U.S., EU Launch "Privacy Shield" Data Transfer Framework, Certification to Begin August 1

U.S. organizations that collect, receive, handle, or process EU citizens' personal data are generally subject to EU privacy and data protection laws.

With the loss of the "Safe Harbor" data transfer framework in October 2015, thousands of U.S. organizations lost their primary mechanism for complying with those EU laws. The new "Privacy Shield" data transfer framework replaces the Safe Harbor and allows U.S. organizations that take part in the Privacy Shield to legally collect and process personal data of EU citizens.

The EU-U.S. Privacy Shield was formally approved on July 12, and the Department of Commerce will begin accepting applications to join the Privacy Shield program starting on August 1. U.S. organizations that wish to participate must:

- implement a data protection policy and practices that comply with the Privacy Shield's requirements;
- clearly display a compliant privacy policy on their website;
- self-certify on an annual basis that they meet all of the Privacy Shield's obligations;
- provide EU citizens the ability to choose whether the organization can share personal data with third parties;
- ensure third parties that receive EU personal data from the organization comply with the Privacy Shield's obligations; and
- respond to privacy-related complaints from EU citizens within 45 days of receipt.

Three Key Takeaways

- The new Privacy Shield offers a straightforward mechanism for organizations to legally transfer EU personal data to the U.S.
- There are specific requirements to join the Privacy Shield program, so compliance may require a change to existing practices and privacy policies.
- Certifying within two months of the effective date offers the benefit of a grace period for third-party relationship requirements.

What Is the Privacy Shield?

The Privacy Shield is a binding data transfer framework that governs the transfer, handling, sharing and use of EU citizens' personal data within the United States. Compared to the Safe Harbor, the Privacy Shield imposes stricter and more comprehensive data protection obligations on U.S. organizations that handle EU personal data.

For more information, please contact any of the following members of Katten's **Privacy, Data and Cybersecurity** practice.

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

Joshua A. Druckerman
+1.212.940.6307
joshua.druckerman@kattenlaw.com

Which Organizations Are Affected?

All U.S. entities—large or small—that process[1] personal data of EU citizens must comply with either the Privacy Shield or another EU-approved data transfer framework, such as model contracts or binding corporate rules (BCR), or otherwise face enforcement actions and liability from individuals and government regulators alike.

The Department of Commerce will serve as the primary regulator of the Privacy Shield program for most U.S. organizations. It will maintain a public list of organizations that have joined the program, and is required to conduct regular reviews of participating organizations to verify and enforce compliance. The Federal Trade Commission (FTC) and the Department of Transportation (DOT) also are empowered to monitor and enforce the Privacy Shield's obligations within their respective areas of authority.

What Obligations Does the Privacy Shield Impose on U.S. Organizations?

The central feature of the Privacy Shield is a self-certification system by which U.S. organizations voluntarily commit to seven Privacy Principles based on the EU Data Protection Directive[2] and, where applicable, additional Supplemental Principles promulgated by the Department of Commerce.[3] These Principles become legally binding and enforceable against organizations that join the Privacy Shield program.

The Privacy Principles include:

- *The Notice Principle*. Organizations must provide clear written notice to individuals before first requesting personal data. The notices must contain a commitment to comply with the Privacy Shield and include certain mandatory disclosures, such as opt-out requirements, the purposes for which personal data is used, dispute resolution mechanisms, and the potential for disclosure to law enforcement agencies.
- *The Choice Principle*. Organizations must provide individuals with the ability to choose whether the organization can disclose personal data to a third party or use it for a "materially different" purpose; obtain opt-in consent before sharing or using certain sensitive personal data; and allow individuals to opt-out of having their personal data used for direct marketing purposes.
- *The Security Principle*. Organizations must take "reasonable and appropriate" measures to protect personal data from loss, misuse, unauthorized access, disclosure, alteration or destruction.
- *The Data Integrity and Purpose Limitation Principle*. Organizations must take reasonable steps to ensure the accuracy, currency and completeness of personal data they process; limit the collection of data to what is relevant and necessary; and only use personal data for the purposes for which it was originally collected (or subsequently authorized).
- *The Access Principle*. In most situations, organizations must provide individuals with the ability to access, correct, amend or delete personal data about them that is inaccurate or has been processed in violation of the Privacy Principles.
- *The Accountability for Onward Transfer Principle*. Organizations may be held liable for any Privacy Shield violations committed by third parties or agents to whom they transfer personal data. Such transfers may only take place for specific limited purposes, and only where there is a contract that provides the same protection as the Privacy Principles. Organizations that certify within the two months of the effective date of the Privacy Shield will have a nine-month grace period from their date of certification to bring existing third party relationships into compliance with this Principle, subject to certain conditions.[4]
- *The Recourse, Enforcement and Liability Principle*. Organizations must provide free, independent and expedited dispute resolution of individual complaints, and must respond to such complaints within 45 days of receipt. Organizations also must designate an external dispute resolution body for the resolution of claims.

---

[1] Processing is broadly defined to include handling, receiving, collecting, sending, using, storing, altering and deleting personally identifiable information.

[2] Commission Implementing Decision, ¶¶ 19–29 (July 12, 2016).

[3] Annexes to the Commission Implementing Decision, pp. 24–46 (July 12, 2016).

[4] Annexes to the Commission Implementing Decision, p. 29 (July 12, 2016).

Why Should U.S. Organizations Consider Joining the Privacy Shield Framework?

The Privacy Shield allows U.S. organizations to legally process EU personal data. U.S. organizations that process EU personal data outside of an approved framework, such as the Privacy Shield, can face significant liability. Sanctions can include civil and/or criminal liability under EU data protection laws, enforcement actions from government agencies, and lawsuits from EU citizens.[5]

Key Considerations for U.S.-Based Organizations

U.S. organizations that collect and process EU personal data and that are not currently a party to an EU-approved data transfer framework should consider taking the following steps to prepare for Privacy Shield implementation:

- review current data management practices, policies and programs and compare them to the requirements contained in the Privacy Shield. In particular, organizations should review arrangements with third parties to ensure compliance with Privacy Shield standards;
- determine the costs, organizational hardships and timeline associated with implementing Privacy Shield requirements;
- create and implement a data management program that complies with the requirements of the Privacy and Supplemental Principles;
- educate and train stakeholders, management, third parties, employees and other professionals on their obligations under the Privacy Shield; and
- conduct either an internal self-assessment or an independent outside assessment of the organization's compliance with the Privacy Shield prior to self-certification.

Finally, it is worth noting that the Privacy Shield faces an uncertain future. EU privacy advocates have threatened to challenge the Privacy Shield in court, arguing that it does not provide sufficient protection for EU citizens' personal privacy, which is the same claim that sank the Safe Harbor. It is unclear whether the Privacy Shield's more robust protections would survive judicial review.

[5] Congress passed the Judicial Redress Act earlier this year, which granted EU citizens the right to enforce EU privacy rights in U.S. courts and extended the rights and protections of the 1974 Privacy Act to EU citizens.