News & Media

The New European Union-U.S. Data Privacy Shield…Is It Right for You?
10/11/2016
Articles & Alerts

U.S. companies with transatlantic operations should carefully balance the need to transfer personal data about European customers and employees from Europe to the U.S. in light of the increased burdens and cost of compliance imposed under the EU-U.S. Privacy Shield (the Privacy Shield).

Before U.S. companies can transfer personal information of citizens of EU member countries (whether those individuals are employees or customers) from Europe to the U.S., they must implement a data transfer mechanism approved by the European Commission to ensure compliance with strict EU data protection laws. The former framework, known as the Safe Harbor, was invalidated by the European Court of Justice last year. In July of 2016, the European Commission approved its successor framework, the Privacy Shield, jointly developed by U.S. Department of Commerce (the DOC) and the European Commission.

Though the Privacy Shield can be viewed as a replacement for the previously invalidated Safe Harbor, its compliance requirements are significantly more onerous. The Privacy Shield requires organizations to self-certify their adherence to seven "core" principles and 16 "supplemental" principles (the Principles) in order to enjoy the benefit of Privacy Shield protection. While the decision to enter the Privacy Shield is voluntary, once an organization self-certifies to the DOC and publicly declares its commitment to adhere to the Principles, it must fully comply with them as a matter of U.S. law. Once a company self-certifies compliance with the Privacy Shield the U.S. Federal Trade Commission (FTC) has jurisdiction over monitoring that compliance and will work with the applicable EU data protection authority to enforce it.

The DOC has committed to "maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the DOC" and declared their commitment to adhere to the Principles (the Privacy Shield List). From the date that the DOC places the organization on the Privacy Shield List, that organization is responsible for providing the benefits of the Privacy Shield to individuals, as outlined in the Principles. If an organization voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the DOC, it will be removed from the Privacy Shield List. Should an organization be removed from the Privacy Shield List, it may no longer rely on the Privacy Shield to receive personal information from the EU without running afoul of EU privacy law.

Companies choosing to self-certify their compliance with the Principles must be willing to adapt their data management practices in the following key areas:

- **Individuals must be accurately and adequately informed about how the organization processes data and personal information**. To this end, the Principles require organizations to include various disclosures and commitments in their privacy policies, including a declaration of the organization's commitment to comply with the Principles and a link to the Privacy Shield Website. Organizations must also provide information regarding: (i) the rights of individuals to access their own personal data; (ii) the organization's requirement to disclose personal information to public authorities under certain circumstances; and (iii) the organization's liability related to transfer of data to third parties. For most companies, this will mean that current privacy policies will have to be updated to reflect this transparency.
- **Organizations must provide free and accessible dispute resolution mechanisms for individuals**. Organizations must respond within 45 days to individuals who bring a complaint related to the management of their personal information directly to the organization. Additionally, organizations must provide, at no cost to the individual, an independent recourse mechanism to efficiently resolve complaints and disputes. Organizations must also commit to binding arbitration at the request of the individual to address any complaint that has not been resolved by other recourse and enforcement mechanisms.

Related Information

Professionals

David A. Gurwin

Adam G. Wicks

Practices

Corporate

Cybersecurity & Data Protection

- **Organizations must ensure accountability for data transferred to third parties**. The Principles contain numerous requirements for organizations who transfer data to third parties, and generally require that data may only be processed by third parties for limited and specific purposes and that the recipient will provide the same protections as the participating organization would under the Principles. Based on the details of a given transfer and recipient, the participating organization must take certain steps to ensure that the third party generally maintains the same level of privacy safeguards as the participating organization.

(For the full text of the detailed Principles, click here).

In addition to the areas above, the Principles impose new administrative requirements, including the following:

- Organizations must cooperate with the DOC by responding promptly to any inquiry or request by the DOC related to the Privacy Shield.
- Organizations must maintain data integrity and purpose limitation by limiting personal information to the information relevant to its purpose and must not retain personal information and data beyond what is necessary.
- An organization must be transparent if it becomes subject to an FTC or court order based on non-compliance, by making public any sections of a compliance or assessment report submitted to the FTC that are related to the Principles.
- Even if an organization leaves the Privacy Shield, it still must annually certify its commitment to apply the Principles to personal information it received when it was participating in the Privacy Shield, for as long as it retains such data.