Akin®

EU-US Privacy Shield Released

Mar 1, 2016

Reading Time : **5 min**

By: Francine E. Friedman, Matthew Thomas (Senior Public Policy Specialist), David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

Under the Privacy Shield, U.S. companies that transfer data to and from the EU will be required to implement a privacy policy that conforms to the privacy principles outlined in the Privacy Shield, to make such policies publicly available, and to annually recertify their compliance with the DOC. While a company's decision to self-certify its adherence to the Privacy Shield principles is initially voluntary, once it does so, its commitment is enforceable under U.S. law by either the Federal Trade Commission or the Department of Transportation, depending on which agency has jurisdiction over the company. The DOC will maintain and publish a listing of all companies that have self-certified their adherence to the Privacy Shield, as well as removing those that voluntarily withdraw, fail recertification or are found to be persistently noncompliant. In cases of persistent noncompliance, the DOC will maintain a list of those companies and the reasons for noncompliance.

In the interim period between the invalidation of the previous Safe Harbor agreement and the implementation of the new Privacy Shield, other means for data transfers between the United States and the EU have been permitted to continue. These include Standard Contractual Clauses and Binding Corporate Rules, which can still be used for personal data transfers to the United States. However, the working group of EU Data Protection Authorities charged with implementing the Privacy Shield have made clear that they intend to review whether these other means remain viable in light of the new protections provided by the Privacy Shield. This review is likely to take place in March.

Privacy Shield Principles

The Privacy Shield puts forward seven primary privacy principles, as well as 16 supplemental principles (collectively, the "Principles"). In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, a company must self-certify its adherence to the Principles to the DOC (or its designee). While decisions by companies to enter into the Privacy Shield are voluntary, compliance is compulsory: companies that self-certify to the DOC and publicly declare their commitment to adhere to the Principles must comply fully with the Principles.

The seven primary principles are:

1. **Notice**: A company must provide individuals with information about its participation in the Privacy Shield, the types of data it collects and the purposes for which such data is used, the identity of any third parties to which such data may be transferred, the right of individuals to access any data collected about themselves, the ability of individuals to limit or tailor the types of data collected about themselves, and an independent dispute resolution mechanism designed to address complaints and provide recourse to individuals free of charge.
2. **Choice**: Companies must provide individuals with the option to choose whether their personal information can be disclosed to a third party or be used for a purpose that is materially different from that for which it was originally collected ("opt-out"). For sensitive information, such as medical, racial/ethnic and religious beliefs, companies must obtain affirmative consent ("opt-in") before transmitting to a third party or for a materially different use.
3. **Accountability for Onward Transfer**: Companies must comply with the notice and choice principles above in order to transfer data to a third party, and they must enter into a contract with the third party stating that such information may be used only for limited and specified purposes consistent with the consent provided by an individual and that the third party will provide the same level of privacy protection under the Principles.
4. **Security**: Companies obtaining, processing and/or disseminating personal information must take reasonable steps to ensure that such information is protected from loss, misuse, unauthorized access, disclosure, alteration or destruction.
5. **Data Integrity and Purpose Limitation**: Collection of personal information must be limited to such information that is relevant for the purposes of processing. A company

may not process information in a way that is incompatible with the purpose for which it has been collected.

6. **Access**: Individuals must be given the ability to access information collected about themselves and have the ability to edit or delete information where it is inaccurate.

7. **Recourse, Enforcement and Liability**: Companies must provide a recourse mechanism to address individual complaints when adherence to the Principles is not followed. This includes, at a minimum, readily available independent recourse mechanisms for investigation of complaints at no cost to the individual, follow-up procedures for verification of attestations and assertions that companies make about their privacy practices, and obligations to remedy problems arising out of failure to comply with the Principles. Companies are obligated to arbitrate claims and follow the terms as of the Arbitral Model (described below), provided that an individual has invoked binding arbitration by delivering notice to the company.

The Supplemental Privacy Principles contain specific requirements relating to especially sensitive information, journalistic exceptions, liabilities for Internet Service Providers, due diligence and audits of adherence to the Principles, the role of EU Data Protection Authorities, and self-certification and compliance verification procedures, as well as greater detail on access, transfer and dispute resolution.

Arbitral Model

The Privacy Shield includes a model for binding arbitration of complaints to disputes raised by EU individuals under the Recourse Principle; however, it is designed as a last-resort option and requires individuals to pursue remedies through other means first. Individuals opting to invoke the arbitration option must have previously raised the complaint directly with the company in question and must have afforded the company the opportunity to resolve the issue within 45 days of the original complaint. The individual must also have made use of the dispute resolution mechanism provided by the company at no cost and must have raised the complaint with an EU Data Protection Authority or the DOC before invoking arbitration. Once these requirements are met, should the individual feel that a suitable remedy has not been made, he or she may invoke binding arbitration proceedings. Under the arbitration option, a Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties involved) will have the authority to impose individual-specific, nonmonetary equitable relief (such as access, correction, deletion or return of the individual's data in question) necessary to

remedy the violation of the Principles with respect to only the individual. These are the only powers of the arbitration panel with respect to remedies.

Next Steps

With the release of the final text of the Privacy Shield, and the adequacy decision issued by the European Commission, a committee composed of representatives of the EU Member States and the EU Data Protection Authorities will be formed and will give their opinion, before a final decision by the EU College of Commissioners. In the meantime, the United States will make the necessary preparations to put in place the Privacy Shield. The decision concluding the final agreement should be adopted by the EU Council after obtaining the consent of the European Parliament.

Categories

Cybersecurity, Privacy & Data Protection

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.