



Jul 14, 2016

Categories:

[Publications](#)

Authors:

[Joseph J. Dehner](#)

It's official – EU approves Privacy Shield

Nine months after the EU-U.S. Safe Harbor Framework for personal data was declared invalid by the EU Court of Justice, EU and U.S. officials announced the approval and adoption of the EU-U.S. Privacy Shield Framework. The Privacy Shield is a negotiated agreement that replaces the Safe Harbor Framework, and provides U.S. companies with a structure for establishing that their collection, use and transfer of personal data of EEA (European Economic Area) citizens is handled in a manner that provides adequate protection as required by EU data privacy laws. It addresses the key concerns voiced by EU officials and others: U.S. assurances concerning bulk data collection for government mass surveillance purposes; a right of redress in the U.S. for EU citizens and mechanisms for that redress; and a requirement for data retention.

The process calls for self-certification in the U.S., much like the Safe Harbor process. Beginning August 1, 2016, companies may begin submitting their self-certifications to the U.S. Department of Commerce. The Privacy Shield Framework consists of four main elements:

- **Privacy Shield Principles.** These principles create a code of conduct and require companies to take action in seven areas that include the FTC's Fair Information Practice Principles, and several others mandated by the EU Data Privacy Directive: notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement, and liability.
- **Oversight and enforcement mechanisms.** The U.S. Department of Commerce has committed to step up its compliance and enforcement activities and conduct regular reviews of companies that have self-certified to the Privacy Shield. The FTC and DOC will be responsible for enforcement according to their jurisdictions, with most companies being subject to FTC enforcement, based upon its enforcement authority under Section 5 of the FTC Act.

- **Ombudsperson.** A position for a new ombudsperson in the U.S. State Department, independent from the intelligence services, will be created to help address EEA citizens' surveillance complaints and issues with respect to personal data transferred under the Privacy Shield for national security reasons.
- **Safeguards and limitations.** Certain U.S. agencies have provided written assurances concerning safeguards and limitations with respect to personal data transferred to the U.S. under the Privacy Shield for national security and law enforcement purposes.

Next Steps

To assist companies with their review of the Privacy Shield Framework and their process of self-certification, the Department of Commerce has published a [Guide to Self-Certification](#).

As companies begin to review their compliance programs, they should take specific steps now, such as determining their eligibility to participate in the Privacy Shield Framework, and updating their privacy notice to comply with the Privacy Shield Principles and state that the organization complies with them. It will be necessary to select, and in some cases to register with, an independent dispute mechanism such as the Council of Better Business Bureaus, TRUSTe, or the AAA. Alternatively, companies can choose to allow their disputes to be resolved in compliance with EU data protection authority (DPA) panels.

The Privacy Shield requires companies to commit to resolve any disputes concerning employee-related data by complying and cooperating with DPA dispute resolution, guidance and panel decisions. In light of the commitment to more rigorous enforcement by the DOC and FTC, companies must establish effective procedures to verify and maintain compliance. Companies will need to designate a Privacy Shield contact within their organization as the first point of contact for Privacy Shield issues. Annual reports of compliance are required.

One cautionary note – the same individual who successfully challenged the now-discarded Safe Harbor Framework, launched court action to challenge the validity of model clauses and Binding Corporate Rules, which have been used as an alternative to the Safe Harbor, and suggested in comments following the European Commission’s announcement of the Privacy Shield that the Privacy Shield was likewise inadequate to protect the privacy of European Economic Area citizens. Nonetheless, Data Privacy Commissioners in EEA countries should honor compliance with the Privacy Shield process, making it highly unlikely that companies pursuing this path would be subject to fines and adverse publicity for data transfer issues if they adopt this new approach and implement it correctly.

For more information, please contact [Jane Hils Shea](#) or [Joe Dehner](#) in Frost Brown Todd’s [Privacy and Information Security Law Practice](#). Mr. Dehner will participate in a major European conference on Data Privacy in late September, presenting the U.S. approach to data privacy in the company of European data privacy commissioners, experts and privacy officers.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.