FOLEY & LARDNER LLP

EU-U.S. Privacy Shield Agreement Released

By Chanley T. Howell, James R. Kalyvas, Sophie Lignier, Steven M. Millendorf, Elizabeth A. Mitro, Eileen R. Ridley, and Aaron K. Tantleff
01 March 2016

Legal News: Privacy, Security & Information Management, Legal News: Technology Transactions & Outsourcing

Quick Read

- The European Commission and the U.S. Department of Commerce released draft documents that will constitute the new Privacy Shield to permit cross-border transfers of personal data between the EU and the United States
- This issue impacts all U.S. businesses that transfer personal data between the EU and the United States
- The framework must still be approved by the data protection regulators representing the 28 EU Member States
- The proposed framework includes the following features:
  - Companies must provide greater transparency with respect to their data collection, use, and sharing practices through more robust and detailed privacy policies
  - Companies handling human resources (employee) data must agree to cooperate and comply with EU Data Protection Authorities (DPAs)
  - Companies transferring personal data to third-party service providers should remain fully responsible for the proper handling of personal data; must conduct appropriate due diligence concerning its service provider; and must properly monitor and remediate any deficiencies of its service providers relating to the handling of personal data
  - Individuals will have the right to file a complaint with respect to the handling of his or her personal data, which must be responded to by the company within 45 days
  - Companies must provide, at no cost to the individual, an alternative dispute resolution mechanism for the resolution of complaints
  - The Federal Trade Commission (FTC) has committed to vigorous enforcement of the Privacy Shield framework, including receiving referrals of complaints from EU DPAs, the Department of Commerce, privacy self-regulatory bodies, and alternative dispute resolution providers
  - EU individuals will be able to pursue legal remedies through private causes of action in U.S. state courts (e.g., misrepresentation and similar types of claims)
  - Companies must commit to binding arbitration before the “Privacy Shield Panel” in the event individual complaints have not been resolved through the companies’ alternative dispute resolution proceedings or other enforcement mechanisms
  - The approval process now moves to the EU Member State DPAs
  - Model Contracts and Binding Corporate Rules are still the only EU approved methods of data transfers at this time
  - Companies should become educated on the current Privacy Shield proposal and continue to closely monitor further developments so that they can move quickly in the event the Privacy Shield is finally approved

On February 29, 2016, the European Commission released the full text of the new EU-U.S. Privacy Shield framework that will govern the transfer of personal data between the European Union and the United States. The documents announcing and comprising the Privacy Shield framework can be found here. The EU and U.S. Department of Commerce previously announced that a new framework for transfers of personal information (also referred to as personal data) from companies in the EU to companies in the U.S. had been agreed upon following the October 2015 ruling from the Court of Justice of the European Union (Court of Justice) that invalidated the existing U.S.-EU Safe Harbor framework. While still in draft form, the adequacy decision issued by the European Commission proposes new limits around the collection and use of personal data by the U.S. government and may provide further guidance to U.S. organizations that wish to use the new framework for trans-border data flows.

Impact to Businesses

While not finalizing the Privacy Shield framework, this is a significant development on the path to doing so. In the event the Privacy Shield is ultimately adopted by all necessary parties, this will remedy the current uncertainty that occurred when the Safe Harbor framework was invalidated. Accordingly, companies should start educating relevant stakeholders now with respect to the proposed requirements of the Privacy Shield, so that in the event it is approved in the same or substantially same form as currently proposed, organizations will be ready to quickly take action should they choose to self-certify under the Privacy Shield. Waiting to consider these issues will only delay companies' ultimate decision and the implementation activities of companies taking advantage of the Privacy Shield.

Privacy Shield Requirements Applicable to U.S. Companies

The Privacy Shield sets forth stronger obligations on U.S. companies to protect the personal data of EU citizens. Companies will self-certify compliance with the Privacy Principles set forth in the Privacy Shield through a public Privacy Shield list maintained by the Department of Commerce, and will need to annually re-certify compliance in order to continue to rely on it for trans-border data flows between Europe and the United States. The Privacy Principles will require companies to take the following affirmative steps:

- **Complaints.** In the event of any complaint by an individual regarding the handling of his or her personal data by a company, whether the complaint is received directly from the individual or through the Department of Commerce, the company must respond to the individual within 45 days.
- **Dispute Resolution.** Companies must provide individuals with access to a free, independent alternative dispute resolution body to resolve disputes regarding the handling of personal data. As such, companies will be required to pay for the alternative dispute resolution proceedings, such as non-binding mediation and mandatory binding arbitration. The Department of Commerce will verify the company's registration with its publicized dispute resolution body. Additionally, companies must agree to submit a recourse mechanism of "last resort" of binding arbitration by the "Privacy Shield Panel," consisting of a pool of arbitrators designated by the Department of Commerce and the European Commission.
- **Human Resources Data.** Companies that handle human resources data from EU citizens must also commit to compliance with advice from the applicable national Data Protection Authority (DPA). This will result in U.S. companies, in effect, being regulated by EU DPAs. As discussed further below, disputes not resolved through negotiation will be subject to resolution through a no-cost mandatory binding arbitration process.
- **Privacy Policies.** A company's privacy policy must notify individuals of the type of data collected, how the data is handled, and available opt-out mechanisms. Companies with online privacy policies must also include the following:
    - A statement of commitment that the company will comply with the Privacy Shield
    - A pledge not to collect more personal information than is needed for its services
    - A point of contact, either within or external to the organization, to handle complaints by individuals
    - Hyperlinks to the Department of Commerce's Privacy Shield website and the website or complaint submission form of the independent dispute resolution body selected
- **Onward (Further) Transfers to Third-Party Service Providers.** In the event a company engages in onward transfers of personal data to third-party service providers, the company will remain fully liable and responsible for the personal data in the hands of subcontractors,

regardless of contractual obligations. A company may only participate in onward transfers where such transfers are appropriately limited and when contractual or other mechanisms provide the same level of protection guaranteed by the Privacy Principles. The Privacy Shield framework further requires companies to conduct due diligence to ensure contractors process personal data in a manner that is consistent with the Privacy Principles; take steps to stop and remediate unauthorized processing of personal data by contractors upon notice; and provide the Department of Commerce with a summary or copy of its contractual privacy protections with a contractor upon request.

Remedies Available to Individuals

In addition to lodging a complaint with the company itself and through the free alternative dispute resolution method, aggrieved individuals may seek redress with the applicable DPA, which will refer any such complaints to the Department of Commerce. Similarly, a company's failure to comply with the ruling of the independent dispute resolution body must be reported by that body to the Department of Commerce and the Federal Trade Commission, or a competent court. In the event of a referral to the Department of Commerce by a DPA, the Department will resolve complaints within 90 days or, in the event it is unable to do so, the complaint may alternatively be referred to the FTC for investigation and resolution. The FTC will prioritize investigations and resolutions of complaints of non-compliance received from the Department of Commerce, independent dispute resolution bodies, and the DPAs, and may enforce compliance through consent orders.

A "last resort" recourse method will be available in the form of binding arbitration by a Privacy Shield Panel that may impose "individual-specific, non-monetary equitable relief" necessary to remedy a company's non-compliance with the Privacy Principles. Companies that certify compliance with the Privacy Shield must participate in any method of redress pursued by an individual, and must respond to requests for compliance information issued through such dispute resolution mechanisms, including requests from the Department of Commerce, FTC, independent dispute resolution bodies, and the DPAs.

Finally, if a company fails to comply with its commitment to respect the Privacy Shield principles and its published privacy policy, individuals may also seek redress under U.S. state laws, such as those providing legal remedies under tort law, misrepresentation, unfair or deceptive acts or practices, and breach of contract.

U.S. Government Surveillance to be Limited Under Framework

The U.S.-EU Safe Harbor framework was invalidated as a result of EU concerns over the National Security Administration's mass data collection program that was revealed by Edward Snowden in 2013. As a result, one of the key objectives of the Privacy Shield framework was to limit the U.S. government's surveillance of EU citizens. The Privacy Shield allows the collection of personal data for national security purposes only when the collection is proportional and limited in scope to address the applicable security risk and balanced against the individual's right to privacy. The Privacy Shield does not prohibit the bulk collection of personal data, but does require that such methods may only be utilized where targeted collection is not possible "due to technical or operational considerations." Under the new framework, EU citizens who seek redress regarding the collection and use of their personal data by the U.S. government may directly complain to a new ombudsperson in the Department of State. The ombudsperson will be independent from the U.S. national security community and will be committed to responding to appropriate complaints or other requests for information submitted by EU citizens.

Additionally, on February 24, 2016, President Obama signed the Judicial Redress Act, which will eventually enable EU citizens to seek remedies for alleged violations by the federal government in U.S. courts. EU citizens (and citizens of other countries/organizations designated in the future by the United States Department of Justice) will be entitled to pursue remedies under the Privacy Act against certain U.S. agencies for the improper handling of personal data in criminal or terror

investigations, including for the improper disclosure of their data. Potential remedies include injunctive relief and monetary damages.

Next Steps

The Article 29 Working Party, a group of regulators representing the 28 EU Member States, must issue its approval of the Privacy Shield before it can be presented to the European Commission for a finding of "adequacy" as required under the EU Data Protection Directive (and as would be required under the forthcoming General Data Protection Regulation). While an adequacy finding by the commission would represent that the safeguards under the new framework are akin to EU data protections, significant criticism of the proposed framework has already come to light.

Members of the European Parliament expressed skepticism about the new agreement's ability to protect the privacy of EU citizens any more than Safe Harbor and withstand judicial scrutiny, while Max Schrems, the Australian privacy activist who filed the complaint that resulted in invalidation of the Safe Harbor framework, and Fanny Hidvegi, an International Privacy Fellow at the Electronic Privacy Information Center (EPIC), along with other activist groups, openly criticized the Privacy Shield and expressed frustration with what they view as unresolved core problems in the framework.

Thus, the Privacy Shield may face an uphill battle before it may be relied upon for the transfer of personal data, and it is prudent for businesses to remain informed, but cautious, while criticism of the Privacy Shield is addressed prior to its acceptance by the European Commission. Furthermore, businesses should be aware that the Court of Justice held that national DPAs may exercise independent oversight to determine the adequacy of privacy protections by data controllers and processors. As such, even if Privacy Shield is ultimately adopted, U.S. companies may still be subject to additional scrutiny regarding data collection and processing activities by the DPAs of different Member States, and may subject U.S. companies to additional requirements, "including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles." This process has shown that the national DPAs have very different stances on privacy, which, as a result, could lead to very different, contrary remedies against the same U.S. company, including the ability to separately investigate and/or block data transfers within their Member State.

Foley will continue to follow developments in the adoption, implementation, and ongoing review of the Privacy Shield, and will provide continuing analysis on best practices for complying with the framework and managing associated responsibilities.

Legal News is part of our ongoing commitment to provide legal insight to our clients and colleagues. If you have any questions about or would like to discuss these topics further, please contact your Foley attorney or the following individuals:

Chanley Howell
Partner
Jacksonville, Florida
904.359.8745
chowell@foley.com

James Kalyvas
Partner
Los Angeles, California
213.972.4542
jkalyvas@foley.com

Eileen Ridley
Partner
San Francisco, California

415.438.6469
eridley@foley.com

Aaron Tantleff
Partner
Chicago, Illinois
312.832.4367
atantleff@foley.com

Sophie Lignier
Of Counsel
Brussels, Belgium
322.787.9700
foley.com/sophie_lignier

Steven Millendorf
Associate
San Diego, California
858.847.6737
smillendorf@foley.com

Elizabeth Mitro
Associate
Boston, Massachusetts
617.502.3287
emitro@foley.com