wiley

ALERT

Looking Ahead to the Privacy Shield

March 3, 2016

The much-anticipated text of the E.U.-U.S. Privacy Shield is finally available, proposing a new framework for transatlantic data flows to replace the invalidated Safe Harbor. E.U. and U.S. negotiators previewed the agreement earlier this month, saying it would create greater obligations on U.S. companies, implement stricter safeguards and enforcement, and provide E.U. citizens several redress possibilities. The actual text of the Privacy Shield bears this out, building on the structure of the original Safe Harbor.

The self-regulatory model that underpinned the original Safe Harbor of 2000 has been largely overtaken. In its place, the Privacy Shield creates a new regulatory landscape defined by much more particular privacy requirements, increased monitoring and enforcement by a more active Department of Commerce, and by a new level of cooperation between U.S. authorities and E.U. data protection authorities (DPAs) to investigate and address complaints. Indeed, companies that certify under the Privacy Shield may find themselves dealing with DPAs exercising new powers and new resources to intrude into the operations of U.S. businesses in an unprecedented manner.

Although release of the Privacy Shield text marks an important step forward, it does not provide any immediate relief to transatlantic businesses for cross-border data transfers. The E.U. Article 29 Working Party will consider the 132-page package released earlier this week at an extraordinary plenary meeting at the end of March and deliver a non-binding opinion on whether it passes muster. The European Commission then must adopt an "adequacy decision" following consultation with a committee of E.U. Member State representatives. Such an "adequacy decision" must have a strong enough foundation to reasonably survive an anticipated challenge before the European

Authors

Daniel P. Brooks
Partner
202.719.4183
dbrooks@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Court of Justice, which invalidated the original Safe Harbor. All told, formal adoption of the Privacy Shield still is at least a month or two away, if not more. In the meantime, transfers based on the Safe Harbor no longer are valid, and at least one German DPA has announced that it is pursuing enforcement proceedings against companies that are continuing to rely on the Safe Harbor for their data transfers.

The European Commission is encouraging eligible U.S. companies to prepare for the Privacy Shield and to be in a position to self-certify as soon as an adequacy decision is adopted. Although privacy obligations would apply immediately upon certification, the Privacy Shield offers companies that certify within the first two months following its effective date a nine-month grace period to bring existing commercial relationships into compliance. Below, we highlight key details of the Privacy Shield text as well as potential pitfalls for U.S. businesses considering certifying under the new framework.

New Obligations on U.S. Companies

Like the original Safe Harbor requirements, the Privacy Shield commitments would become legally binding on a participating U.S. company by virtue of that company's public representations. For example, a U.S. company might engage in prohibited unfair or deceptive trade practices subject to Federal Trade Commission (FTC) enforcement if the company failed to uphold its representations that participation in the Privacy Shield would require.

Thus, it is extremely significant that the Privacy Shield will require U.S. companies to make a much longer and more specific list of public representations than the original Safe Harbor – in privacy notices given to individuals, in posted privacy policies, and in certifications to the Department of Commerce. Such disclosures will include explicit acquiescence to the enforcement jurisdiction of the FTC or other participating federal agency. Any U.S. company considering the Privacy Shield should ensure that its data handling practices are prepared to follow this expanded list of representations, which will require:

- Constraining handling of personal information only to the "purposes" described in a privacy representation;
- Constraining third parties' handling of disclosed personal information only to the "limited and specified" purposes for disclosure described in a representation;
- A mechanism to support an E.U. individual's "right to access personal data," which can be a complex, burdensome and expensive process;
- Various logistical and procedural specifics, including contact information for complaints, as well as the mechanisms adopted for compliance verification and an independent recourse mechanism; and
- Keeping a company's public privacy policy up to date and "comprehensive" concerning its status under the Privacy Shield.

Also, updating contracts with agents and other third parties likely will be a significant undertaking for new Privacy Shield participants that disclose E.U. personal information. While contracts were often required under the original Safe Harbor, the list of necessary provisions has expanded under the Privacy Shield. Among other

things, contracts must specify the "limited" purposes for which personal data may be used; ensure privacy protection equivalent to the Privacy Shield standards; address reasonable security; and be responsive when individual consent is present or lacking. Further, third parties easily could be implicated in data access requests, compliance verification, and dispute resolution, and contracts should provide accordingly. Notably, contractual provisions with third parties could be demanded by the Commerce Department, which conceivably could be shared with E.U. privacy regulators. U.S. companies should be aware that they could be held responsible if a third parties' use of E.U. personal information does not meet the Privacy Shield requirements.

Protections of E.U. Citizens' Privacy Rights

In a significant break from the invalidated Safe Harbor, the Privacy Shield offers a variety of new mechanisms for E.U. individuals to raise complaints regarding the treatment of their personal information. Individuals may file complaints directly with U.S. companies, make use of free alternative dispute resolution services provided by the relevant company, or file complaints directly with their local DPA, who will work with the Department of Commerce and the FTC to investigate and resolve complaints. As a last resort, individuals also may file complaints with the Privacy Shield Panel.

The Privacy Shield encourages E.U. consumers to raise complaints first with the relevant U.S. company and requires companies to respond to consumer complaints within forty-five days. The Privacy Shield also requires companies to make available independent recourse mechanisms for investigating and resolving consumer complaints and for awarding damages, where applicable. Such mechanisms must be available at no cost to the individual. Examples of acceptable independent enforcement mechanisms include: (i) compliance with privacy programs developed by the private sector that incorporate the Privacy Shield Principles into their rules and include effective enforcement mechanisms; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; and (iii) cooperation with E.U. data protection authorities.

According to the Privacy Shield text, dispute resolution bodies "should look into each complaint received from individuals unless they are obviously unfounded or frivolous" and impose appropriate remedies to reverse the effects of non-compliance, ensure that future processing by the company will conform to the Privacy Shield Principles, and cease the processing of the personal data of the individual who brought the complaint. Sanctions "should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances" and may also include "compensation for losses incurred as a result of non-compliance and injunctive awards."

As a last resort, the Privacy Shield provides an arbitration option for determining whether a U.S. company has violated its obligations under the Principles and whether any such violation remains fully or partially unremedied. Prior to invoking the arbitration option, an individual first must (1) raise the claimed violation directly with the company and allow the company an opportunity to resolve the issue within the 45-day period described above; (2) make use of the company's independent recourse mechanism; and (3) raise the issue through the individual's data protection authority to the Department of Commerce, which will (at no cost to the

individual) use its best efforts to resolve the issue.

The arbitration panel will have authority to impose only non-monetary equitable relief (*e.g.*, access, correction, deletion, or return of the individual's data) and may not award damages, costs, or fees. The parties to a dispute will select up to three arbitrators from a pool of 20 arbitrators designated by the Department of Commerce and the European Commission. Arbitral decisions will be binding on the parties and will preclude relief for the same claim in another forum, though an individual will be permitted to seek damages in court if the non-monetary equitable relief does not fully remedy the violation. Both individuals and U.S. companies will be permitted to seek judicial review and enforcement of arbitral decisions under the Federal Arbitration Act. The costs of arbitration will be paid for through annual contributions by Privacy Shield companies, though each party will be responsible for its own attorney's fees.

Strengthened Oversight by the Department of Commerce

According to a letter from Under Secretary for International Trade Stefan Selig, the Department of Commerce has increased the resources that will be devoted to the administration and supervision of the Privacy Shield program, including doubling the number of staff. New resources will be used to verify self-certification requirements; expand efforts to follow up with companies that are removed from the Privacy Shield list; search for and address false claims of participation; and conduct compliance reviews and assessments of the program. The Department of Commerce's specific role in administering the Privacy Shield is detailed below.

- For the first time, the Department of Commerce will verify a U.S. company's self-certification prior to placing the company on the Privacy Shield List. The Department of Commerce will verify, for example, that the company has provided all required information to self-certify; identified the specific statutory body that has jurisdiction to hear any claims against the company; identified the method of verification of assuring compliance with the principles (*e.g.*, in-house or third party); and identified the independent recourse mechanism that is available to investigate and resolve complaints, among other details. The Department of Commerce also will work with independent recourse mechanisms to verify that Privacy Shield companies have in fact registered with the relevant mechanism indicated in their self-certification submissions.
- The Department of Commerce will expand efforts to follow up with companies that have been removed from the Privacy Shield List, including by notifying companies that are removed from the Privacy Shield list that they are not entitled to retain E.U. citizens' data collected under the Privacy Shield and by sending questionnaires to companies whose self-certifications lapse or who voluntarily withdraw from the Privacy Shield to verify whether the company will return, delete, or continue to apply the Principles to personal information received while participating in the program.
- The Department of Commerce will actively search for and address false claims of participation, including verifying that companies that withdraw from the Privacy Shield, fail to recertify, or are removed for failing to comply remove any references to the Privacy Shield from any published privacy policy.

- The Department of Commerce will conduct *ex officio* compliance reviews and assessments of the program, including through detailed questionnaires to participating companies.

The FTC also retains its primary enforcement role under the Privacy Shield and may undertake investigations on its own initiative or based on referrals of non-compliance. FTC investigations will seek to determine whether a Privacy Shield company violated Section 5 of the FTC Act or other relevant laws.

Increased Cooperation with E.U. DPAs

The Privacy Shield lays the groundwork for strengthened cooperation between the Department of Commerce and E.U. DPAs. Specifically, the Department of Commerce will establish a dedicated contact to act as a liaison with DPAs. In instances where a DPA believes that a U.S. company is not complying with the Principles, the DPA can refer the case to the liaison for further review. In addition, the Privacy Shield documentation envisions that the liaison will "assist DPAs seeking information related to a specific company's self-certification or previous participation in the program." The scope of this information gathering is unclear, but it suggests that E.U. DPAs will have new access to a wider set of information concerning U.S. companies certified under the Safe Harbor.

The Privacy Shield also requires the Department of Commerce to provide updates to E.U. DPAs within 90 days of receiving a complaint, and to provide an annual report analyzing the complaints it receives each year. The new framework envisions annual meetings between the Department of Commerce and the European Commission, interested DPAs, and "appropriate representatives from the Article 29 Working Party" to review the functioning of the Privacy Shield. E.U. DPAs also will play a role in designating arbitrators for the Privacy Shield Panel.

* * *

We will continue to monitor relevant developments and offer additional guidance, should the Privacy Shield ultimately be adopted.