Hogan Lovells
CHRONICLE of DATA PROTECTION
PRIVACY & INFORMATION SECURITY NEWS & TRENDS

Posted on July 28th, 2016 By Bret Cohen, Katherine Gasztonyi, Julie Brill and Eduardo Ustaran

Navigating from Safe Harbor to Privacy Shield: A Primer

In less than one week, on August 1, U.S. companies may begin to submit self-certifications to the EU-U.S. Privacy Shield framework at www.privacyshield.gov. Those companies that previously certified to the predecessor Safe Harbor framework are in a particularly good position to certify to the Privacy Shield, which built upon Safe Harbor's core principles by adding meaningful substantive and procedural privacy protections for EU individuals.

A company seeking to transition from Safe Harbor to Privacy Shield will need to engage in three general steps: (1) update its external-facing privacy policy; (2) develop internal policies and procedures to comply with new Privacy Shield requirements; and (3) more closely manage its relationships with third parties that will receive or have access to Privacy Shield data, including ensuring contracts with those third parties meet new Privacy Shield requirements. We summarize these three steps, as well as additional procedural requirements that will affect the impact of Privacy Shield on U.S. businesses compared to Safe Harbor.

Update External-Facing Privacy Policy

With respect to individual notice, Safe Harbor merely stated that a participating organization was required to "inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure."

Privacy Shield's notice requirements are much more specific and in line with the requirements under the forthcoming EU General Data Protection Regulation, listing 13 different requirements for participants to include in their published Privacy Shield privacy notices, including:

- a statement that the organization is subject to the enforcement powers of the FTC (or other applicable regulatory authority);
- identification of the dispute resolution body designated to address complaints, including a hyperlink to the dispute resolution body's website and a statement that the use of the process is free of charge;
- an explanation of the possibility for EU individuals to invoke binding arbitration;
- an explanation that the organization may have a requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security requirements; and

- a note that the organization remains liable for the processing of personal information in some circumstances when that personal information is transferred to third parties.

When moving to Privacy Shield, organizations also should remember to remove public-facing representations about their Safe Harbor compliance, including their Safe Harbor privacy notices.

Internal Policies and Procedures

Privacy Shield adds a number of new substantive and procedural requirements that may require companies to adopt and implement new internal policies and procedures prior to certification, including:

- *Data retention procedures:* A key change from Safe Harbor (and from the originally released version of Privacy Shield) is the adoption of a new data retention requirement. This requirement limits the retention of personally identifiable information "only for as long as it serves a purpose of processing" for which it was collected or subsequently authorized by the individual. To comply with Privacy Shield, and organization must take "reasonable and appropriate measures" to comply with this provision, most likely by adopting and enforcing a data retention and destruction policy. There are exceptions allowing the retention of information for the purposes of journalism, scientific research, statistical analysis, and other similar purposes.
- *Recordkeeping:* Privacy Shield requires companies to retain their records of the implementation of their Privacy Shield practices and to make these records available to regulators the course of an investigation. This is very much in line with the documentation and accountability obligations introduced by the EU General Data Protection Regulation.
- *Training:* Organizations should update internal training documents and conduct training on the newly required Privacy Shield processes and procedures.

Third Party Disclosures

One of the most prominent changes to the EU-U.S. data transfer regime under Privacy Shield is the treatment of onward transfers of EU personal information to third parties. Unlike under Safe Harbor, companies certified to Privacy Shield are required to enter into written contracts with all third parties that receive Privacy Shield information. Privacy Shield sets forth specific contractual requirements for transfers to third-party controllers (i.e., third parties that are authorized to use the information for their own purposes), and others for transfers to agents (i.e., third parties that act only on behalf of and on the instruction of the company).

To transition from Safe Harbor to Privacy Shield, an organization should identify all third parties to which it transfers data that would fall under the framework. Then, it should distinguish controllers from agents and take steps to make sure that each relationship conforms to the Privacy Shield's contracting requirements. For example, the transferring organization must:

- only transfer data to third parties for limited and specified purposes;
- upon notice that a third party is unable to continue to sufficiently protect the privacy of the personal information (notice which must be provided under the agreement), take reasonable and appropriate steps to stop and remediate unauthorized processing;
- take reasonable and appropriate steps to ensure that agents effectively process the personal information in a manner consistent with the organization's Privacy Shield obligations, which effectively requires some measure of privacy and security diligence; and
- upon request, provide a summary or a representative copy of the relevant privacy provisions of its contracts with agents to the Department of Commerce.

Significantly, Privacy Shield explicitly states that organizations remain liable for their agents' failure to comply with the principles unless the organization can show it was not responsible for the event giving rise to the violation, so Privacy Shield members may wish to review these contracts for appropriate risk-shifting provisions as well.

Companies that certify to Privacy Shield by the end of September will have until the end of April 2017 to conform third-party contracts to these new requirements; otherwise, the expectation is that all of an organization's third-party contracts will conform to these requirements upon certification.

Additional Procedural Requirements

Privacy Shield also introduced a number of procedural requirements to support the enforcement of the program that were not present under Safe Harbor. Some of these requirements may impact compliance risks, including:

- As with under Safe Harbor, companies certified to Privacy Shield must maintain a third-party dispute resolution body to assess any complaints from EU individuals that the parties were unable to resolve on their own. Unlike Safe Harbor, Privacy Shield expressly calls for these bodies to award damages "where the applicable law or private-sector initiatives so provide." Privacy Shield also allows individuals as a last resort to appeal decisions of this independent dispute resolution body to a newly constituted "Privacy Shield Panel," which will have the authority to arbitrate disputes and impose individual-specific, nonmonetary equitable relief to remedy noncompliance with Privacy Shield.
- Organizations and their independent dispute resolution bodies must "respond promptly" to inquiries and requests by the Department of Commerce, which for its part is obligated to pass along complaints referred by EU data protection authorities. Privacy Shield contemplates that EU residents may file complaints directly with their local data protection authorities, which will work with the Department of Commerce and the Federal Trade Commission to investigate and resolve these complaints.
- When an organization becomes subject to a FTC or court order based on noncompliance with Privacy Shield, it will be required to make public "any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC," to the extent consistent with confidentiality requirements. These types of internal compliance reports are typically demanded by the FTC as part of any privacy compliance investigation, so under this rule these reports could later become public.
- The Department of Commerce is required to, in consultation with EU data protection authorities where appropriate, conduct periodic *ex officio* reviews of an organization's Privacy Shield compliance when either (1) it receives "specific non-frivolous complaints" about the organization's compliance; (2) the organization does not respond satisfactorily to inquiries by the Department; or (3) there exists "credible evidence" that the organization does not comply with Privacy Shield. Under Safe Harbor, there was no affirmative obligation for U.S. government authorities to investigate complaints. Given EU concerns about enforcement, it is likely that Privacy Shield participants will face greater compliance scrutiny than under Safe Harbor.

* * * * *

Organizations compliant with the Safe Harbor principles, and which regularly verified that compliance, should not have a tough time transitioning over to the Privacy Shield, with retains many of the same requirements. That said, Privacy Shield requires that companies be compliant with Privacy Shield before certification, so companies that plan on certifying at the outset of the program should confirm that they can comply with the new obligations under Privacy Shield, most of which are set forth above. Our practical advice to any organization aiming to join the Privacy Shield is to carry out a swift internal compliance assessment, draw up a well-structured compliance strategy prioritizing the obligations set out above, and implement that strategy in a consistent way across the organization.

Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004 | USA
Phone: +1 202 637 5600
Fax: +1 202 637 5910

Hogan Lovells International LLP
Atlantic House
Holborn Viaduct
London EC1A 2FG
United Kingdom

Phone: +44 20 7296 2000
Fax: +44 20 7296 2001

Copyright © 2016, Hogan Lovells US LLP and Hogan Lovells International LLP. All Rights Reserved.