Privacy Shield is final: What it means for businesses

Data Protection, Privacy and Security Alert

21 JUL 2016

The US Department of Commerce announces that it will begin accepting applications for Privacy Shield certifications beginning on August 1.

For US organizations collecting personal data from the EU, the past year has been an anxious one, as the European Court of Justice invalidated the EU-US Safe Harbor program in October 2015 and the terms of a far-reaching General Data Protection Regulation (GDPR) have been promulgated to replace the EU's 1995 Data Protection Directive. Among other things, one of the major impacts of the GDPR – when it takes effect in May 2018 – is that it will apply to US businesses that sell to, make services available to or somehow target data subjects in the EU – even if those US businesses have no operations or affiliates in the EU. With the GDPR looming, the issue of cross border data transfers and the significance of the Privacy Shield program for US businesses are likely to become even more relevant.

On July 12, the European Commission and the US Department of Commerce issued the final text of the replacement for the defunct Safe Harbor program. The new program, dubbed Privacy Shield, is effective immediately but will not become truly operational until the Commerce Department starts accepting certifications on August 1, 2016. The new program is

also almost certain to be subject to a challenge before the European Court of Justice, and so the long-term viability of Privacy Shield is somewhat uncertain.

The main questions for US-based organizations are: how does this final version of Privacy Shield differ from the initial version; what practical steps can companies take to prepare for certification; and should companies certify to Privacy Shield or rely on an alternative data transfer mechanism, such as standard contractual clauses?

Key differences between Privacy Shield and Safe Harbor

There are several ways in which Privacy Shield is more than simply an updated version of Safe Harbor.

1. The public-facing statements that companies must make (e.g., in website privacy policies) must be significantly more detailed. No longer will a simple statement of participation in the program be acceptable. Instead, the statement must include a clear explanation of compliance with the Privacy Shield principles. In these privacy statements, a company also must describe an individual's rights under the program, such as how the program's enforcement bodies function, a new arbitration right and the company's liability for non-compliant onward transfers.
2. With respect to such onward transfers, the conditions for such data sharing have been tightened. A company only will be able to transfer personal data to a third party for limited, specified purposes consistent with the purposes for collection that the company specified in the privacy statement provided to data subjects. Consequently, companies will need to include more specific contractual obligations than required under Safe Harbor in their contracts with service providers and other third parties to which they disclose or transfer personal data. The Commerce Department also has the right to require a company to provide a summary of the company's onward transfer contractual provisions for the Department's review. As an incentive to early adopters, those joining Privacy Shield within the first two months will have nine months from certification to bring their partner contracts into compliance.
3. The Commerce Department and Federal Trade Commission will have greater obligations to vet applicants and ongoing audit rights, and FTC will have a "wall of shame" identifying Privacy Shield violations. There will be ongoing obligations for former Privacy Shield participants, as Commerce and the FTC will continue to monitor the compliant handling of data collected under the program, even after a company withdraws from the program.
4. There are new redress avenues for individuals complaining about either a company's misuse of data collected under Privacy Shield or the US government's access to or surveillance of personal data.

Changes in the final version of Privacy Shield

The European Commission and the Commerce Department negotiated several substantive changes to the Privacy Shield program in response to comments and feedback on the initial version. From a business perspective, some of the more notable changes are the following:

- The Privacy Shield principles have been expanded in some significant ways. For example, while the Data Integrity/Purpose Limitation principles now include details for data retention and compatible uses, the Accountability principle now makes sure that if a third party is unable to apply the same level of protection that the Privacy Shield certified organization has promised, that organization must provide notice to affected individuals.
- The redress process has been explained in greater detail, such that even though there are different avenues for a data subject to initiate a complaint, the text makes clear that there is a certain logical order and data subjects cannot simply bypass an initial approach to the company itself to discuss concerns.
- The Commerce Department's role has been expanded, as discussed above, and key to this will be the ability to conduct ongoing audits of program participants. These reviews will typically be via questionnaires, although Commerce will also be able to audit on the basis of specific complaints or other evidence of non-compliance.

Steps to take in preparation for Privacy Shield

All companies considering Privacy Shield will benefit from the following steps:

- **Develop, maintain and follow a meaningful and compliant privacy policy**. The seven privacy principles are largely the same as under Safe Harbor, even if the level of detail and content requirements of Privacy Shield will require operational attention to ensure consistency with the policy.
- **Secure personal data and ensure the ability to restrict secondary uses**. While Privacy Shield does not provide

great detail on the required administrative, technical or physical safeguards, there are numerous internationally recognized frameworks for doing this. The secondary use restrictions in Privacy Shield will require additional consideration, as personal data will need to be reasonably de-identified before being subject to data analytics or other secondary uses.

- **Review existing data sharing agreements with vendors, partners and third parties** to ensure that they limit data uses to specified purposes.
- **Review internal training content** to ensure that it reflects updated policy and procedures under the Privacy Shield program.
- **Collect the full set of program documentation in preparation for a Privacy Shield application**. Contrary to the Safe Harbor program, in which application-stage vetting was quite limited, Commerce has committed that it will be significantly more involved to ensure that applicants not only have documentation fulfilling the requirements, but that the applicant properly applies the relevant policies and procedures.

It's important to keep in mind that the Privacy Shield, like Safe Harbor before it, applies only to data transfers from the EU to the US and does not affect processing within the EU. Beginning in May 2018, the GDPR will govern data processing within the EU. More to the point, an organization participating in Privacy Shield will still need to conduct a separate analysis of how its operations conform to the GDPR – especially with respect to the processing and transfer of employee data.

Potential challenges and momentum

The *Schrems* case not only struck down the validity of the European Commission's adequacy determination approving Safe Harbor, but also bolstered the standing of EU DPAs to challenge the basis of other mechanisms to transfer personal data from the EU. In the preamble to the Commission's adequacy determination, the Commission made clear that its decisions are as a matter of law binding upon the EU member states, while acknowledging the role that DPAs can play in identifying imperfect implementation by Privacy Shield participants.

Litigation challenging Privacy Shield is all but certain. In the meantime, the Article 29 Working Party is expected to release its opinion on the final Privacy Shield Program by the end of July 2016.

But even if the Article 29 Working Party issues a positive review, several DPAs are likely to criticize the arrangement and might even argue in favor of invalidation in an ECJ hearing, as they did against the Safe Harbor. Furthermore, Mr. Schrems himself will likely initiate proceedings again.

Some organizations will find this uncertainty about the fate or validity of Privacy Shield reason to adopt a wait and see approach. They may, for example, prefer to execute or continue to use standard contractual clauses (SCC) instead of certifying to Privacy Shield. SCC present their own challenges. SCC have themselves already been challenged in a case referred by the Irish DPA to the ECJ. In some EU member states they must be submitted to a DPA for prior approval, slowing down their use. SCC must also be executed with or on behalf of each EU data exporter, which can be operationally difficult in some circumstances -- Privacy Shield, like Safe Harbor, will reduce this paperwork burden. Yet SCC may remain the only option when transfers are from the EU to countries other than the US that are not subject to an adequacy decision.

Several high-profile companies have already announced their support of and participation in Privacy Shield once it is operational. In the end, we expect that Privacy Shield will be successful (at least for the medium-term, and hopefully for the long term) if the Commission and the various DPAs work together with the Commerce Department toward the operational effectiveness of the program.

For more information, please contact us via dataprivacy@dlapiper.com.