April 14, 2016

Weil

Alert
Cybersecurity, Data Privacy & Information Management

Preparing for Adequacy Under the Privacy Shield

By Randi W. Singer and Cheri E. Bessellieu

U.S. companies must comply with European data protection laws when collecting, using, and storing personal information about European citizens. Among other things, they must ensure an "adequate" level of protection for any personal information of European citizens transferred outside of Europe to the United States. In 2000, the U.S. worked with European authorities to develop a set of guidelines known as the EU-U.S. Safe Harbor, and the European Commission (EC) determined that U.S. companies who complied with the Safe Harbor would be deemed to provide an "adequate level of protection" consistent with the requirements of the European Data Protection Directive 95/46/EC. As a result, many U.S. companies sought to comply with European data protection law by self-certifying under the Safe Harbor. The European Court of Justice, however, disrupted this approach when, on October 6, 2015, it ruled that compliance with the Safe Harbor did not ensure adequate protection of personal information. Following the invalidation of the Safe Harbor, the EC and the United States Department of Commerce have agreed to a revised set of principles and procedures known as the EU-U.S. Privacy Shield, designed to ensure that compliant companies provide an adequate level of protection for the personal information of EU citizens.

The EC published a draft adequacy decision concerning the Privacy Shield, and the United States Department of Commerce released the text of the Privacy Shield on February 29, 2016. While the proposed framework carries over many obligations from the Safe Harbor, the Privacy Shield includes heightened obligations for U.S. companies that transfer personal information about EU citizens to the United States. These include:

- broader certification requirements;
- clearer notice obligations;
- stricter contractual obligations in vendor agreements;
- narrower use of data where appropriate;
- greater access rights for individuals; and
- broad mechanisms for recourse and dispute resolution.

Before U.S. companies can rely on the Privacy Shield, EU privacy regulators, including a committee of representatives of the EU Member States, will issue opinions regarding the adequacy of the principles, and the College of EU Commissioners must formally adopt the Privacy Shield. While the necessary procedural hurdles for the Privacy Shield are addressed, U.S. companies can take preliminary steps to align their internal privacy practices and standards with the obligations set forth in the draft Privacy Shield.

Update the Privacy Notice

Before a company can self-certify under the Privacy Shield with the Department of Commerce, it will need a privacy notice that reflects the principles of the Privacy Shield. A qualifying privacy notice must clearly explain what personal information the company collects, how it uses such personal information, the scope of third-party access to the personal information, and the company's liability for personal information transferred by third parties. In addition, the Privacy Shield requires companies to have a privacy notice that explains how individuals can access their personal information, as well as control the use and dissemination of their personal information. Companies should develop and explain procedures for users to lodge complaints under the Privacy Shield, identify the appropriate independent dispute resolution body, and disclose the possibility that an individual may have the right to binding arbitration. The privacy notice also should disclose that the company is certified under the Privacy Shield, as well as provide a link to or web address for the Department of Commerce's list of organizations that have self-certified under the Privacy Shield.

As with the Safe Harbor, the proposed Privacy Shield requires companies to explain how individuals can opt-out if they do not want a company to share their personal information with a third party or use it beyond the scope of the disclosed intended purposes. Companies must obtain affirmative consent before disclosing certain sensitive information. The privacy notice should reflect mechanisms for both.

Consider Third Parties Carefully and Revisit Third-Party Agreements

A company that certifies under the Privacy Shield and relies on third parties to transfer personal information from Europe will be liable for the third party's failure to comply with the principles of the Privacy Shield unless the company can show that it is not responsible for the event in question. Of course, this makes the selection of third parties who transfer personal information on behalf of a company and negotiations with those third parties significantly more important. During the vetting process, companies should take a close look at how the third party processes, stores, uses, and protects personal information, and whether the third party has procedures in place to ensure compliance with the principles of the Privacy Shield. Companies may consider hiring consultants to aid in the vetting process.

Companies may need to renegotiate existing third-party agreements or enter into new ones in order to ensure compliance, both of which may require significant time and effort. Under the Privacy Shield, third-party agreements should clearly state that any transfer of personal information is limited to the scope of use to which the individual consented, that

the third party itself complies with the principles of the Privacy Shield, and that the company will use reasonable and appropriate steps to ensure the third party complies with those principles. Compliance may require companies to intervene and/or change the way third parties process personal information if the third party's use is without authorization or beyond what is authorized. Companies also should consider appropriate monitoring mechanisms and evaluate whether additional internal resources are needed to monitor. Because the Department of Commerce can request copies of third-party agreements, companies should ensure that the agreed-upon provisions comply with the principles set forth in the Privacy Shield.

Companies who certify under the Privacy Shield within two months of its effective date will have, at most, a nine-month period to ensure that third-party agreements conform to the principles of the Privacy Shield. For those companies that certify after the initial two-month period, the requirements for third-party agreements apply immediately upon certification.

Only Collect and Use What Is Needed

Under the Privacy Shield, data must be "relevant for the purposes of processing", companies must collect only information that is relevant and they must reasonably ensure that "data is reliable for its intended use, accurate, complete, and current." These requirements continue to apply to data collected under the Privacy Shield even after certification expires. Companies should carefully consider the reasons why they are collecting data and whether it is possible to achieve the same goals with less information. This may also be a good time to begin discussions regarding the reliability, accuracy, and completeness of data. If a company reasonably stores personal information for long periods of time, it may want to consider whether to allow or require individuals to periodically update their information.

Develop a Path to Greater Access

Can individuals access, correct, or amend their personal information or delete inaccurate information? Can individuals confirm whether their personal information is being processed and, if so, processed lawfully? While the Privacy Shield provides certain limitations surrounding sensitive business information and personal rights, companies that certify under the Privacy Shield must answer yes to these questions. Companies should explore their current technological and personnel capabilities to provide individuals the access that the Privacy Shield requires. In appropriate circumstances, companies may charge individuals a non-excessive fee for access to their personal information.

Prepare to Resolve Disputes

The Privacy Shield's most significant departure from the Safe Harbor involves complaints from and procedural remedies available to individuals concerning the processing of their personal information. Privacy Shield-compliant companies must implement processes to provide recourse for individuals, develop procedures to verify that their privacy practices comply with the principles of the Privacy Shield, and provide remedies for noncompliance. Companies should consider what third-party dispute resolution bodies might be

appropriate for use as an independent recourse mechanism, or whether they prefer to appoint a panel of Data Protection Authorities from EU Member States. Under both scenarios, the decision maker must have the authority to require a company to compensate the user, suspend certification, or cause the company to disclose any non-compliance to the public. A company will need to allocate internal resources to respond to complaints within 45 days and resolve any disputes at the company's cost. If a company elects to receive advice from Data Protection Authorities and does not adhere to such advice, the FTC can hear the dispute. A company's failure to comply with advice from a dispute resolution body would go before the appropriate Data Protection Authority, and after that, if necessary, the Department of Commerce. The final mechanism available after exhausting all others is binding arbitration.

Conclusion

While U.S. companies wait for a final decision regarding the Privacy Shield, it is not too early to start thinking about steps to take and changes to implement now, as full compliance with the current version of the Privacy Shield will entail significantly more work than compliance with the U.S.-E.U. Safe Harbor did for most companies. In addition, preparing to comply will strengthen a company's privacy and data security measures.

Cybersecurity, Data Privacy & Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy & Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein (NY)	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi W. Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

Contributing Authors:

Randi W. Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Cheri E. Bessellieu (NY)	Bio Page	cheri.bessellieu@weil.com	+1 212 310 8957