LEGAL UPDATE

October 2016

By: Jeffrey Johnson, Francesca Djerejian, and Michelle Arbour of Pryor Cashman's Corporate Group

EUROPEAN UNION AND THE UNITED STATES IMPLEMENT NEW JOINT PRIVACY SHIELD

On July 12, 2016, the EU Commission formally launched a new transatlantic data transfer framework, known as the EU-U.S. Privacy Shield, to replace the U.S.-EU Safe Harbor, which was invalidated in October of last year by the Court of Justice of the European Union due to concerns that the U.S. failed to meet adequate standards of data protection. The Privacy Shield provides a framework for transatlantic exchanges of personal data for commercial purposes between the EU and the U.S. Its compliance requirements are significantly more burdensome than the U.S.-EU Safe Harbor, and as a result, multinational companies are wary of the new scheme: A survey conducted in June and July found that of the 600 privacy professionals surveyed, only 34% said they plan to rely on the Privacy Shield. In addition, although the Article 29 Working Party, Europe's governing body of privacy authorities, has broadly welcomed the Privacy Shield, it has expressed concern that several of its recommended changes were not adopted. The Working Party has indicated, however, that the new regime will not be up for challenge by the European Court of Justice until a year from now.

In the meantime, the Privacy Shield has been formally implemented and its key principles delineated, which include:

- The appointment of an independent ombudsman by the State Department whose role will be to oversee access by U.S. intelligence officials and address EU citizen complaints regarding the use of their personal data by national intelligence authorities;
- Greater oversight of transatlantic data transfers by the U.S. Department of Commerce and Federal Trade Commission (FTC), including greater cooperation with European Data Protection authorities;
- The requirement that all U.S. companies importing personal data from Europe publish their data protection policies with the Department of Commerce, which are to include clearer terms of use for data processing and onward transfers of data to third parties;
- An obligation that companies that have self-certified provide information to individuals concerning the processing of their personal data;
- The imposition of annual fees by participating companies to support the operation of the Privacy Shield framework;
- The requirement that any U.S. company transferring human resources data from Europe formally commit to comply with decisions by the European Data Protection authorities;
- The imposition of liability for onward transfers and a requirement that any third party data transfers comply with notice and consent requirements, and that companies entering into contracts with third-party controllers ensure such transfers are compliant with the new principles;
- Provisions aimed at limiting the access of U.S. public officials and law enforcement agencies to the personal data of EU citizens, including clarification that bulk collection of data can only be used under exceptional circumstances such as terrorism probes and must be deployed as narrowly as possible;
- The imposition of more robust redress mechanisms, including referrals by European Data Protection authorities to the Department of Commerce and the FTC; and
- The availability of dispute resolution mechanisms for any individuals who feel their data has been misused under the Privacy Shield scheme (at no added cost to such individuals), including the right to make complaints directly to national data protection authorities.

The now-abolished Safe Harbor Framework had allowed U.S. companies to transfer, process and store data outside of the EU in a manner consistent with the EU Data Protection Directive, provided such companies "self-certified" to the U.S. Department of Commerce that they were compliant with EU data privacy standards. Under the new EU-U.S. Privacy Shield, self-certification alone will no longer be a sufficient means of ensuring compliance with the EU data privacy requirements as companies will have to publish their data protection policies and be subject to more direct scrutiny by the U.S. Department of Commerce and the FTC.

Privacy Shield Compliance and Self-Certification

The U.S. Department of Commerce began accepting self-certifications to the Privacy Shield on August 1. A U.S.-based organization can voluntarily join the Privacy Shield program, at which point the commitment to comply with the Privacy Shield Principles becomes enforceable under U.S. law. Companies will have to carefully review the more robust requirements of the Privacy Shield, in addition to rules regarding processing activities, before making the determination to self-certify.

Upon self-certifying, companies must take the following steps:

1. **Confirm the Organization's Eligibility to Participate in the Privacy Shield.** Any U.S. organization that is subject to the jurisdiction of the FTC or the Department of Transportation (DOT) may participate in the Privacy Shield. Both the FTC and the DOT have committed that they will enforce the Privacy Shield framework.
2. **Develop a Privacy Shield-Compliant Privacy Policy Statement.** There are several steps an organization must take to develop a privacy shield-compliant privacy policy. First, it must ensure that the organization's privacy policy conforms to the Privacy Shield Principles. To do this, the organization's privacy policy must be clear and concise, and must reflect the organization's information handling practices as well as the choices the organization offers individuals with respect to the use and disclosure of their personal information. Second, the privacy policy must specifically state that it adheres to the Privacy Shield Principles. Third, the privacy policy must identify the organization's independent recourse mechanism, and if the organization's privacy policy is available online, it must include a hyperlink to the website of the independent recourse mechanism. Fourth, the organization must provide an accurate location of its privacy policy and make it publicly available. If the organization has a public website, that website should provide the web address where the privacy policy is available.
3. **Identify the Organization's Independent Recourse Mechanism.** Organizations that self-certify must provide an independent recourse mechanism for individuals to investigate unresolved complaints at no additional cost.
4. **Ensure that the Organization's Verification Mechanism is in Place.** Organizations must also ensure they have procedures in place to verify compliance. To do this, the organization may use either a self-assessment or an outside/third-party assessment program.
5. **Designate a Contact within the Organization Regarding Privacy Shield.** Organizations must provide contact information for the individual that handles questions, complaints, access requests, and any other issues arising under the Privacy Shield. This individual can be the corporate officer that is certifying the organization's compliance with the Framework or another official within the organization.

Once a company self-certifies, it must also take measures to ensure it can comply and implement the above-listed principles. In addition, participants will be required to re-certify on an annual basis. Companies that opt not to self-certify have continued to rely on other legal mechanisms such as the EU standard contractual clauses (SCC) and the limited exceptions set out in Article 25(2) of the EU Protection Directive. However, these companies risk transmitting data between the EU and the U.S. that is not consistent with the EU standards, in which event EU authorities may charge penalties for failure to comply with EU privacy standards. These administrative fines could be as high as 4 percent of the company's gross worldwide revenue or €20 million, whichever is greater.

Now that the EU-U.S. Privacy Shield has taken effect, U.S. companies should assess the adequacy of their data protection policies and the best way to ensure compliance. More specifically, U.S. companies that transfer personal data collected in the EU to the U.S. or other non-EU countries will have

to seriously reevaluate their data protection policies in the context of a new enforcement regime. In addition, U.S. companies should carefully consider whether their data transfer activity warrants self-certification given the substantially more robust requirements imposed by the Privacy Shield. Companies wary of the new regime may opt not to self-certify, but these companies run the risk of not being in compliance with EU standards.

***

For more information, please contact Jeffrey Johnson, jjohnson@pryorcashman.com, of Pryor Cashman's Corporate Group.