October 18, 2016

EU-US Privacy Shield: What You Need to Know for Transatlantic Data Transfers

Karen H Bromberg, Partner
Duane A Cranston, Associate

The flow of data across international borders is crucial to commerce in today's global economy. After last year's invalidation of the Safe Harbor framework, which enabled companies to transfer personal data from the EU to the US by self-certifying that they complied with the EU's stricter privacy standards, businesses were left scratching their heads. EU law dictates that organizations that want to transfer data outside the EU can only do so with adequate privacy protection. But the privacy protection provided by the US has been deemed inadequate, and Safe Harbor, upon which thousands of companies across the world relied for their transatlantic business, has been ruled invalid.

After nine months of uncertainty as to how companies could transfer personal information without running afoul of the EU Data Protection Directive ("EU Directive"), in August 2016, the EU Commission ("EC") finally adopted a new mechanism for the transfer of personal data from the European Union to the United States, branded the "EU-US Privacy Shield" ("Privacy Shield").

What is the Privacy Shield?

The Privacy Shield is a voluntary program which enables its participants to transfer European personal data from the EU to the US so long as the enrollees self-certify that they are in compliance with its principles. Although participation is voluntary, once an organization commits to comply with the program, that commitment is enforceable under US Law and may be enforced by the Federal Trade Commission and the Department of Transportation. The Privacy Shield replaces the Safe Harbor program and has a number of new substantive requirements that companies should carefully consider before signing up to the framework.

The Privacy Shield imposes stronger obligations on US companies to protect Europeans' personal data than its predecessor, Safe Harbor. The rules around disclosures, oversight, data retention, security, notice, and processing are specific and targeted, and the agreement now includes options for individual redress. Among other things, the Privacy Shield requires companies to arbitrate claims with complaining EU individuals who have exhausted prior avenues, and to pay an annual fee to fund arbitration costs. The program is also subject to annual review. According to the EC, it "requires the US to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities."

Technology giants Google, Microsoft and Dropbox are several of the companies that have recently signed up to the framework, taking advantage of the pre-October 1, 2016 grace period which allows them nine months to review and update third-party contracts for compliance with the Privacy Shield principles.

How does the Privacy Shield work?

As of August 1, 2016, the Department of Commerce instituted an online certification process for companies wishing to sign up to the framework (view here). The submission is reviewed by the Department of Commerce and either approved or subjected to further information requests.

In order to be able to certify, companies must have a privacy policy in line with the program's seven privacy principles including notice, accountability for onward transfer, access, choice, security, data integrity and purpose limitation, and recourse, enforcement and liability for non-compliance (the "Privacy Principles"). Supplemental principles include, without limitation, handling of sensitive data, secondary liability, performing due diligence and conducting audits, the role of the data protection authorities, self-certification, verification, obligatory contracts for onward transfers, dispute resolution and enforcement, publicly available information and access requests by public authorities. Participants must renew their "membership" in the Privacy Shield program on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

The Privacy Shield's requirements apply immediately upon a participant's certification with the Department of Commerce. Before self-certifying, a company will need to do the following:

- Confirm that the company is eligible to participate in the privacy shield (*i.e.,* that the company is engaged in an industry regulated by the Federal Trade Commission, which would exclude banks, telecommunications companies, transportation companies and most insurance companies, among other industries);

- Develop and implement a privacy policy statement that complies with the Privacy Principles and other requirements of the Privacy Shield program;

- Identify and implement a mechanism to investigate and resolve complaints at no cost to an individual complainant. Companies may utilize dispute resolution programs such as those administered by the Council of Better Business Bureaus, TRUSTe, and the American Arbitration Association, among others (*note:* if a company's self-certification also covers personal information on its past or present employees, these companies must also agree to comply with the relevant EU data protection authorities in connection with such information);

- Verify that the dispute resolution mechanism has been implemented, either through the company's own self-assessment or using an outside assessment program; and

- Designate a company contact to address question, complaints, access requests, and any other issues relating to the Privacy Shield program.

Conclusion

US companies will need to carefully assess self-compliance with the Privacy Principles before signing up to the framework, particularly in view of the EU's increased attention to the issue of privacy as a paramount policy concern of international data transfers. Participants must review their existing privacy policy and ensure that it is updated and in line with the Privacy Shield's requirements.

Best practices dictate that companies should consult with a data privacy attorney prior to applying in order to understand the new regulatory requirements governing the use and treatment of personal data received from the EU, including the program's privacy principles, as well as the access, security and recourse mechanisms that participants must provide to individuals in the EU and to assess whether signing on to the framework is a sensible solution for the company.

About the Authors:

Karen Bromberg is the head of the firm's Intellectual Property and Technology group. Karen is a Certified Information Privacy Professional (CIPP) with certifications covering both U.S. and European privacy law. She advises clients on a broad range of privacy and data protection matters, including privacy policies and procedures, regulatory investigations, global compliance, cross-border data transfers, cybersecurity and network intrusion issues, and contractual issues involving privacy and security with an emphasis on litigation avoidance.

Contact Karen

Duane Cranston serves as outside general counsel for a number of early to mid-stage companies in industries ranging from technology to healthcare, representing clients in data privacy, intellectual property licensing, commercial transactions, and employment matters. He counsels employers on employment issues including the development of employment policies related to insider trading and data privacy. Duane is a Certified Information Privacy Professional/United States (CIPP/US) through the International Association of Privacy Professionals.

Contact Duane

About Cohen & Gresser:

We are an international law firm with offices in New York, Paris, Seoul, and Washington, D.C. Founded in 2002, we have been recognized in *Chambers USA*, *Legal 500*, and *Benchmark Litigation*, and have grown to nearly seventy lawyers in six practice areas: Litigation and Arbitration, Intellectual Property and Technology, White Collar Defense, Corporate, Tax, and Employment Law.

New York | Paris | Seoul | Washington DC