Privacy in the European Union: A Data Safekeeping Revolution

by Daniel A. Cotter[1]

In 1995, the European Union (the EU) brought to the forefront the issues of privacy and the individual’s right to protection of their sensitive information, when it adopted “Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (the EU Data Protection Directive). A version of the EU Data Protection Directive was implemented in each EU country. The EU’s history of strong commitment to privacy and human rights law is reflected in the EU Data Protection Directive, which was the first major privacy law of its kind. The U.S. Congress subsequently enacted the Health Insurance and Portability and Accountability Act of 1996 and, in 1999, Congress passed the Gramm–Leach–Bliley Act, which governs privacy obligations for financial institutions.

On January 25, 2012, the EU introduced a new privacy regulation, known as the General Data Protection Regulation (the EU GDP Regulation), that superseded the EU Data Protection Directive in May 2018.[2] Companies must review the new EU GDP Regulation and revise their privacy programs to comply with the EU GDP Regulation, even if they are US–only companies. As was the case in 1995, the EU may be on the forefront of more restrictive privacy regulations than the U.S.

The U.S. Safe Harbor

On July 26, 2000, the EU issued European Commission’s Decision 2000/520/EC
“on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce” (the U.S. Safe Harbor). The Safe Harbor Privacy Principles (the principles) were developed between 1998 and 2000, and were designed to put in place systems to prevent accidental disclosure of private information from companies in the EU or U.S. The principles included seven requirements:

1. **Notice.** Individuals must be provided information about their data and how it is being collected and used.

2. **Choice.** Individuals must have the ability to opt out of the collection and transfer of data to third parties.

3. **Onward transfer.** Transferring data to third parties may only occur if the third party to whom the data will be transferred also adheres to the principles.

4. **Security.** Reasonable efforts must be made by the recipient of private information to protect it against loss.

5. **Data integrity.** Data must have integrity (i.e., be relevant and reliable for the purpose for which it was collected).

6. **Access.** Individuals must have the ability to access information about themselves and correct or delete it.

7. **Enforcement.** There must be effective means of enforcing the principles.

U.S. companies that complied with the principles and appropriately answered a series of questions could self-certify compliance and thereby be eligible for the U.S. Safe Harbor and safely transfer EU data to the U.S.

**Invalidation of the Safe Harbor**

On October 6, 2015, the Court of Justice of the EU declared the U.S. Safe Harbor framework invalid, citing the “massive and indiscriminate surveillance” conducted by the U.S.[3] The Court of Justice’s decision left many U.S. companies with little guidance or protection for their EU data practices. On February 29, 2016, the European Commission published a series of documents
detailing the new Privacy Shield framework. The European Commission adopted the framework on July 12, 2016.[4] The Privacy Shield framework requirements are detailed in the EU-U.S. Privacy Shield Principles (the Privacy Shield Principles).[5] Although the Privacy Shield Principles follow the same seven requirements found in the old Safe Harbor Principles, there are significant differences between the U.S. Safe Harbor framework and the new Privacy Shield framework.

Although the specific differences are beyond the scope of this article, the new Privacy Shield framework provides for significantly enhanced notice obligations. U.S. companies wishing to avail themselves of the Privacy Shield will have to inform individuals about 13 aspects of the company’s privacy practices, including:

1. Participation in the Privacy Shield, with a link to the listing of all U.S. companies that have self-certified compliance with the Privacy Shield Principles (i.e., the Privacy Shield List).
2. What types of data the company collects and which subsidiaries or affiliates of the company also adhere to the Privacy Shield Principles.
3. Commitment to strictly adhere to the Privacy Shield Principles for all EU data collected.
4. The purposes for which the company collects and uses the data.
5. The independent dispute resolution body to which complaints and disputes will be submitted for resolution.

The Privacy Shield Principles are substantially more detailed and onerous than the notice requirements provided for in the Safe Harbor Principles.

Significant changes were also made to consumers’ choices. Individuals are given the ability to prevent their personal information from being disclosed to third parties. For sensitive information (defined as “personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual”), the individual must affirmatively permit either the disclosure of sensitive information to a third party, or the use of this information for purposes substantially different from the original collection purpose. The broad definition of sensitive information,
as well as the obligations on a US company participating in the Privacy Shield, make compliance with these obligations more burdensome than compliance with the Safe Harbor Principles. EU individuals also have enhanced redress options at their disposal.

U.S. companies will have additional compliance obligations to be able to avail themselves of the Privacy Shield safe harbor protections. A detailed explanation of those obligations can be found at the Department of Commerce’s Privacy Shield website, at .

This document is only available to subscribers. Please log in or purchase access

Purchase Login