COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Privacy in the European Union: A Data Safekeeping Revolution

By Daniel A. Cotter[1]

In 1995, the European Union (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 then 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25, 2012, the EU introduced a new privacy regulation, known as the General Data Protection Regulation (GDPR), that superseded the EU Data Protection Directive in May 2018.[2] If not already accomplished, companies must review the GDPR and revise their privacy programs to comply with it, even if they are US-only companies.

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 US Department of Commerce" (the U.S. Safe Harbor). The Safe Harbor privacy principles were developed between 1998 and 2000; they were designed to put in place systems to prevent accidental disclosure of private information from companies in the EU or US. 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.

US 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 US.

Invalidation of the Safe Harbor and Privacy Shield Frameworks

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 US.[3] The Court of Justice's decision left many US companies with little guidance or protection for their EU data practices. The European Commission adopted a new Privacy Shield framework on July 12, 2016. The U.S. International Trade Administration published a notice to announce the availability of the Privacy Shield framework on August 2, 2016.[4]

However, on July 16, 2020, the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield framework in a court decision.[5] The U.S. Department of Commerce and the European Commission initiated discussions to determine the possibility for an enhanced EU-U.S. Privacy Shield framework;[6] however, no potential replacement has been outlined between the EU and the US to date. Until there is a new framework, United States companies may use standard contractual clauses (SCCs) to permit the onward transfer of EU[7] citizens' data to the US. On June 7, 2021, the European Commission adopted two new sets of SCCs. In March 2022, the EU and the United States announced a new Trans-Atlantic Privacy Framework.[8] The framework must go through a number of regulatory approvals before it becomes effective.