CORPORATE COUNSEL
An ALM Website
corpcounsel.com | September 29, 2016

Trans-Atlantic Compliance: What U.S. Businesses Need to Know

From the Experts

Jayne Rothman

A complicated picture just got more complex. The trans-Atlantic transfer of personal data between the European Union and the United States is now governed by new data privacy compliance obligations following an October 2015 ruling that invalidated the previous Safe Harbor privacy accord. For U.S. businesses, this means in-house counsel teams need to learn and adhere to a new set of rules and a new set of standards.

Unlike the Safe Harbor framework, the Privacy Shield is the first time that the United States has provided written assurance that it will provide safeguards, oversight, redress processes and defined limitations on public authorities' accessing of personal data. The Privacy Shield framework includes significant advancements to improve transparency on personal data use. It also strengthens the protections afforded to participating companies and informs EU individuals more comprehensively about their rights under the program.

But it is not without its critics. There are concerns about unfettered access to consumer data by intelligence and law enforcement officials. And the fact that the program is subject to annual review has led to questions over whether the law could change on a regular basis, or, as happened last autumn, get struck down altogether.

To join the Privacy Shield, a U.S.-based company will be required to register and self-certify to the U.S. Department of Commerce and publicly commit to comply with the requirements of the new framework. These requirements for participating companies (participants) include but are not limited to:

• NOTICE: Participants must review, update and publicize their privacy policies online and declare their commitment to comply with Privacy Shield and the specific notice requirements of the new framework.

• DISPUTE RESOLUTION: EU individuals whose data is being

processed by participants may lodge a complaint directly with a participant, which must respond to the complaint within 45 days. Participants must provide, without cost to the EU individuals, independent recourse mechanisms to investigate and expeditiously respond to such complaints. Participants must also commit to binding arbitration, at the EU individual's request, to address complaints that have not otherwise been resolved through the processes set forth in the framework.

• COOPERATION WITH DEPARTMENT OF COMMERCE: Participants must cooperate and respond promptly with the U.S. Department of Commerce to resolve complaints submitted by EU individuals (which can also be submitted by these individuals to their local data protection authorities, or DPAs).

• PURPOSE LIMITATION: Similar to the Safe Harbor framework, participants must limit personal information to that which is relevant for processing and pertains to the original purpose for which it was collected (absent subsequent consent by the individual).

• ONWARD TRANSFERS: Participants must enter into contracts with third-party controllers and processors, regardless of location, to ensure adherence to the Privacy Shield framework and principles, including the consent provided by the EU individual to the processing of his or her personal data.

• ACCESS: EU individuals have a right to know if participants are processing their personal data, and may modify correct or delete it under certain circumstances (such as when the data is inaccurate or is processed in violation of the requirements of the Privacy Shield).

Once a U.S.-based company commits to the Privacy Shield framework, the commitment will be enforceable under U.S. law and will remain enforceable regarding any personal data processed during the self-certification period, even if a company is no longer a participating company.

Best Practice Guidelines

Although the EU commission's adequacy decision represents a milestone achievement toward a more unified system of laws and regulations for processing and protecting personal data between the EU and the U.S., detractors and skeptics remain vocal about the shortcomings of the new framework. The Privacy Shield will likely be challenged by activists and ruled upon by European courts, including the Court of Justice of the European Union. Other EU-U.S. data protection and compliance-related issues to be addressed will also focus on the impacts to the Privacy Shield and compliance in general resulting from "Brexit" and the upcoming implementation of the EU General Data Protection Regulation in May 2018.

Companies processing personal data of EU citizens need to undertake privacy impact assessments to analyze what personally identifiable information is collected, used, processed and shared, to understand and appropriately remediate compliance gaps and to make intelligent risk-related decisions with the next three-year horizon in mind. Organizations conducting data transfers involving personal data from the EU are tasked with identifying and implementing a robust plan with built-in contingencies, if the horizon should suddenly change. In addition, the Article 29 Working Party has confirmed that the use of model contracts or binding corporate rules can still be used for transfers of personal data from the EU to the U.S.

Companies involved in the transfer of personal data from the EU to the U.S. should review their policies and procedures in light of these new developments, especially regarding the new General Data Protection Regulation, as it will impact not only companies that operate in the EU, but those that do business with EU consumers.

Jayne Rothman *is senior vice president and general counsel at Epiq Systems, where she has served as senior legal adviser since 2006. She manages matters that include mergers and acquisitions, corporate governance, commercial transactions, litigation and risk and compliance. Rothman is a frequent speaker and author on the topics of enterprise risk management and data privacy.*