PUBLICATION

Uncertainty Abounds After EU High Court Invalidates EU-U.S. Safe Harbor Framework

Authors: Alisa L. Chestler
October 07, 2015

On October 6, 2015, the Court of Justice of the European Union declared invalid the more than 15-year-old EU-U.S. Safe Harbor Framework. Thousands of U.S. businesses have complied with, and thus relied upon, the Safe Harbor Framework to ensure that transfers of employee, consumer, user and other personal data from the EU to the U.S. for storage or processing are compliant with the EU's strict data privacy rules. However, now with the EU high court's judgment, there is significant uncertainty on both sides of the Atlantic, as stakeholders must assess the operational, practical and legal implications of EU-to-U.S. data transfers in the absence of the protections of the Safe Harbor Framework.

Background

Under the EU Data Protection Directive, transfers of personal data from the EU to a non-EU country are prohibited unless the country can assure an adequate level of protection for the data. Given the differing approaches taken by the EU and U.S. on data protection, the United States Department of Commerce, in consultation with the European Commission, developed the Safe Harbor Framework as a mechanism to address the EU law's adequacy standard. U.S. businesses voluntarily participate in the Framework and thereby comply with its terms. In July 2000, the European Commission issued a decision approving the Safe Harbor Framework.

The Safe Harbor Framework provided a number of significant benefits to both U.S. and EU organizations. Not the least of these benefits was the assurance that all 28 EU Member States would be bound by the European Commission's finding that the U.S. – through the Safe Harbor Framework – provides an adequate level of privacy protections. This particular benefit, and now ultimately the entirety of the Safe Harbor Framework, was challenged by an individual who complained to the Irish data protection authority that, given the exposés from Edward Snowden concerning the activities of the U.S. intelligence service, the laws and practices, including the Safe Harbor Framework, offer no real protection against intelligence surveillance by the U.S. government. The Irish data protection authority initially rejected the complaint citing the European Commission's July 2000 decision affirming the Safe Harbor Framework. The Irish high court, however, brought the case up for review by the EU Court of Justice. The EU high court's decision yesterday invalidated the European Commission's July 2000 decision on grounds that the European Commission lacks authority to override EU Member States' ability to investigate whether a non-EU country satisfies the EU Data Protection Directive standard for "adequacy" of data protections or to determine whether to suspend further transfers of data.

Implications

The implications of the decision are as numerous as they are uncertain. First, the most resounding implication is that companies currently operating under the Safe Harbor Framework may be subject to claims that data transfers are unlawful under the EU laws and subject to suspension of data transfers by EU Member State data protection authorities. It remains to be seen, however, whether and how EU Member State data protection authorities will proceed or respond to complaints, or whether companies will be given a grace period to effectuate changes.

Second, U.S. companies seeking to engage in data transfers involving EU data could now be required to comply with a patchwork of differing privacy requirements across EU Member States, or be subject to different or inconsistent determinations by data protection authorities regarding the adequacy of protections.

Third, it remains uncertain whether the alternative mechanisms for assuring compliance with the adequacy standards might ultimately suffer the same fate as the Safe Harbor Framework. Other mechanisms, for instance, include adopting "Binding Corporate Rules" (BCRs). These are contractual mechanisms for ensuring compliance which also may not protect against intelligence surveillance activities.

Fourth, the abrogation of the current Safe Harbor Framework comes as the United States and European Commission have been working for the past two years on improvements to the current structure. It is now unclear whether those efforts can or will bear fruit. In a press release issued on October 6, 2015, the U.S. Secretary of Commerce, Penny Pritzker, expressed disappointment in the decision and urged swift adoption of the updated Safe Harbor Framework. She stated:

We are prepared to work with the European Commission to address uncertainty created by the court decision so that the thousands of U.S. and EU businesses that have complied in good faith with the Safe Harbor and provided robust protection of EU citizens' privacy in accordance with the Framework's principles can continue to grow the world's digital economy.

What Can Be Done Now

Despite the uncertainties, there are steps companies can take in the short term that will help support compliance going forward. For instance, companies should consider:

- Assessing the nature and scope of the organization's reliance on the Safe Harbor Framework for data transfers.
- Analyzing whether any alternative mechanisms for data transfer compliance are viable for your organization.
- Determining whether containment of all or some data within the EU is feasible for the organization.
- Assessing contractual commitments the organization has made or others have made to the organization based on Safe Harbor compliance and determining whether other contractual terms can be inserted (e.g., BCRs).

If you have questions regarding the EU-U.S. Safe Harbor Framework or the implications of the EU high court decision on your organization, please contact Alisa Chestler ;or any member of the Firm's Privacy and Information Security Team.