Privacy Shield Adopted, But Uncertainty Remains

Thursday, July 14, 2016

Yesterday, the European Commission adopted the EU-US Privacy Shield, a framework designed to replace the invalidated Safe Harbor program. In theory, the Privacy Shield offers its adherents a relatively simple, straightforward way to legally transfer personal data from the EU to the US. In reality, however, the Privacy Shield is likely to face legal challenges that may hinder its ability to serve as a reliable means of legal transfer, at least for the immediate future.

As we’ve covered previously, details of the Privacy Shield first emerged back in February, when the European Commission announced that EU and US officials had reached an agreement on a successor to the Safe Harbor scheme. It was no surprise that in the wake of the Schrems decision – which essentially ended the Safe Harbor program based on concerns about US government surveillance of individuals’ personal data – the Privacy Shield would require US companies to meet “stronger obligations” to protect Europeans’ personal data, while the Department of Commerce and Federal Trade Commission would have to engage in “stronger monitoring and enforcement” of companies’ data protection practices. Additional details became available over the course of the next few months and are summarized here.

Despite these inclusions, many in the European community remained skeptical of the Privacy Shield’s purported protections. The Article 29 Working Party, for example, voiced its “strong concerns” about the adequacy of the program, based largely upon its fear of the potential for “massive and indiscriminate collection of personal data.”
Nevertheless, the European Commission adopted the Privacy Shield in an effort to facilitate EU-to-US data flows, reasoning that the “new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers.”

Companies will be able to self-certify their compliance with the Privacy Shield beginning on August 1. As with the Safe Harbor program, companies that are subject to the jurisdiction of the Federal Trade Commission or Department of Transportation are eligible to participate in the Privacy Shield program and may self-certify via the Department of Commerce’s website. Many companies undoubtedly are ready to jump at the opportunity to self-certify their compliance with the Privacy Shield, especially because that self-certification means that they have an adequate legal basis for engaging in transatlantic data transfers and do not need to rely on mechanisms that may be more onerous and/or expensive to implement, such as standard contractual clauses or binding corporate rules.

However, relying on self-certification still poses some risks. Much of the upheaval that has been taking place in EU data protection law over the past year is the result of the revelations regarding the extent of the US government’s surveillance of personal data. Many in Europe – including privacy advocates and even some data protection authorities – are wary of any mechanism that allows data transfers to the US because they believe that the transferred data simply will not be protected from the eyes of the US government. Regardless of how many protections it has in place, the Privacy Shield is unlikely to alleviate these deep-seated concerns, and is therefore likely to face legal challenges in the coming months. A decision invalidating the Privacy Shield, similar to the Schrems decision that did away with the Safe Harbor, would require those companies that had self-certified to scramble to implement standard contractual clauses or binding corporate rules in order to continue importing personal data from the EU. Accordingly, many companies may choose to wait until the effects of self-certification earn a greater degree of legal certainty.

© 2019 Proskauer Rose LLP.

Source URL: https://www.natlawreview.com/article/privacy-shield-adopted-uncertainty-remains