Strategic Perspectives

Wolters Kluwer

July 17, 2018

Privacy Shield Goes the Way of Safe Harbor: Neither a Ship nor Armor Will Suffice

By Cynthia J. Cole and Neil Coulson, Baker Botts LLP*

This is the first in a two-part article series by Cynthia J. Cole and Neil Coulson on the future of cross border transfers of personal data under the General Data Protection Regulation if Privacy Shield disappears from the adequacy landscape for international transfers.

The European Union ("EU") imposes strict requirements on entities that collect personal data from individuals residing in the European Economic Area ("EEA") and then transfer that data to a non-EEA country. The recent General Data Protection Regulation ("GDPR"), adopted in 2016 and effective on May 25, 2018, only permits cross-border transfers to cou ntries or territories with a legal regime that provides an "adequate" level of personal data protection, as determined by the European Commission ("EC").

The United States is not deemed as having "adequate" laws and practices in place for the protection of personal data and thus, companies who transfer personal data from the EEA to the United States must rely on alternative options. One such mechanism is the EU-U.S. Privacy Shield. However, the future of the Privacy Shield as it currently exists is uncertain, as on June 12, 2018, the Civil Liberties committee of the European Parliament (LIBE) passed a resolution calling for its suspension and on July 5, 2018, the European Parliament plenary adopted the resolution. If the European Commission rescinds the Privacy Shield as an adequate data protection mechanism, U.S. companies will be left with very few options under which to conduct cross-border transfers of data originating in the EEA, two of which are: "Binding Corporate Rules" ("BCRs") and "Model Clauses" (also called "standard contractual clauses").

This article generally describes the Privacy Shield, explains why it will likely be rescinded in the near future, and in the second part, generally describes the two alternative options available to U.S. companies that want to directly or indirectly transfer personal data originating in the European Economic Area ("EEA") to countries outside the EEA (to what the GDPR refers to as "third countries"), in a manner that complies with the GDPR.[1]

---

* Baker Botts partner **Neil Coulson** is the Department Chair – Intellectual Property in London and Moscow. **Cynthia J. Cole** is Special Counsel in Palo Alto in Baker Botts' corporate, technology and privacy and data security practice groups.

1 This document does not attempt to describe the full scope of the GDPR's cross-border transfer requirements or how companies can comply with the GDPR's numerous other requirements. This document is not intended to constitute legal advice and should not be relied on as such.

The EU-U.S. Privacy Shield regime currently allows certified companies to engage in cross-border transfer of personal data between the EEA and the U.S. The EU-U.S. Privacy Shield is an agreement between the European Commission and the U.S. Department of Commerce that allows cross-border transfers if such transfers meet a certain set of requirements. It was first adopted in July 2016 as a replacement to the Safe Harbor arrangement, which was a prior data transfer agreement between the two entities that was invalidated by the EU's Court of Justice in 2015. The Privacy Shield allows U.S. companies to self-certify that they will adequately protect personal data in accordance with an EU data subject's fundamental rights and the GDPR.

The EU-U.S. Privacy Shield is likely to be suspended in 2018 in light of the European Parliament's view that it is inadequate to protect the personal information of European data subjects. The Privacy Shield framework is reviewed by the European Commission on a yearly basis. In 2017, the first annual report suggested that the framework ensured an adequate level of personal data protection, although certain areas could be improved. On June 12, 2018, LIBE voted on a resolution to suspend the Privacy Shield, primarily because the U.S. was not adequately enforcing the required protections (the European Commission has long been calling for a permanent ombudsman to be appointed to oversee the enforcement in the U.S. of EU residents' data subject rights). On July 5, 2018, the European Parliament plenary adopted the LIBE's resolution calling on the United States to show compliance by September 1, 2018. The European Commission has scheduled its second annual review of Privacy Shield for October 2018 and has so far adopted a position whereby it is committed to a fully functioning Privacy Shield, in cooperation with the United States. But the pressure is now on the Commission from the European Parliament.

The committee alleged that the U.S. does not adequately enforce the protections that the Privacy Shield requires of U.S. companies. The resolution says that there is insufficient oversight of the certification process and, in general, a lack of supervision. Delays in investigation of companies that may have misused personal data or otherwise breached the Privacy Shield regulations are a massive concern. According to the European Parliament website, several MEPs (members of the European Parliament) called for re-evaluation of the Privacy Shield after issues surfaced publicly in early 2018 showing that prominent Privacy Shield-certified companies were not, in fact, compliant. In particular, MEPs criticized the U.S. for failing to take swift action following revelations of misuse. And MEPs called for companies that have revealed violations of the regulation to be removed from the Privacy Shield list altogether.

There were also questions raised about the rights of access to personal data. MEPs were concerned that personal data transferred from the EEA to the U.S. could be collected and accessed indiscriminately by U.S. public authorities or law enforcement. In particular, the resolution noted that there are no "concrete assurances of not conducting mass and indiscriminate collection of personal data (bulk collection)." Such bulk collection of personal data and communications of non-U.S. individuals is still possible for law enforcement purposes under a very permissible U.S. standard and not the more restrictive EU standard. In addition, the resolution noted that how the Privacy Shield applies to processors of personal data (agents of the companies controlling the data) is not explicitly stated.

In short, the resolution called into question the very framework of the Privacy Shield regulations and alleged that a failure to enforce the Privacy Shield is a failure on the part of the U.S. to protect the fundamental rights of EU residents. If the Privacy Shield is not adequately enforced, it says, then the protections it affords are in name only.

Suspension of the Privacy Shield means currently-certified U.S. companies could no longer use it to conduct cross-border transfers of personal data originating in the EEA. The resolution calls for suspension unless the U.S. demonstrates, by September 1, 2018, that it is adequately enforcing the Privacy Shield's framework. Now that the European Parliament has adopted the resolution the European Commission will be under more pressure in its annual Privacy Shield review in October 2018. If Privacy Shield is revoked, U.S. companies that are currently certified under the Privacy Shield will no longer be able to use it as a valid mechanism for cross-border transfer of personal data out of the EEA.

September 1, 2018, is a very tight deadline, coming on the heels of the whirlwind of data privacy compliance for May 25, 2018. U.S. companies should start sooner rather than later to protect the personal data they are currently collecting and processing and be ready with alternate mechanisms for cross border transfers. In our second article, we will explore two alternative solutions, Binding Corporate Rules ("BCRs") and Model Clauses. BCRs are internal regulations that a company must enact and agree to be bound by. Model Clauses are contractual clauses that the European Commission has decided provide sufficient protections for the transferred data.