JULY 17, 2020

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

Shielded No Longer: Top EU Court Invalidates Privacy Shield Framework and Clarifies Use of Standard Contractual Clauses as Bases for EU-U.S. Data Transfers

Yesterday, the Court of Justice of the European Union (CJEU) issued its long-awaited opinion in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (*Schrems II*), a landmark case challenging the continued legitimacy of Standard Contractual Clauses agreements as a basis for transferring the personal data of EU residents to the United States, and also calling into question the validity of a data-recipient's adherence to the Privacy Shield Framework as a valid transfer mechanism. The verdict: **Privacy Shield is out, but Standard Contractual Clauses are still in—with some caveats.**

Overview of Data-Transfer Mechanisms: The Privacy Shield Framework and Standard Contractual Clauses Agreements

The General Data Protection Regulation (GDPR) is the European Union's comprehensive data privacy and protection regulation. Europe's privacy rules have global reach, imposing a number of obligations and restrictions not only on organizations located in the EU, but also on any organization that targets goods or services to, or monitors the behavior of, EU residents, as well as on those who process the personal data of EU residents on behalf of EU data controllers.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Kate Paine
Associate
813.202.7151
kpaine@shb.com

One such restriction is a prohibition on transferring personal data outside of the EU, absent a valid prescribed mechanism for doing so. Perhaps the most straightforward mechanism is the existence of an "adequacy decision"—a formal decision by the European Commission that a "country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection." Where such a decision exists, transferring personal data from the EU does not require any additional authorization—although the GDPR may still impose other disclosure requirements.

Another transfer mechanism commonly used by U.S. companies is a Standard Contractual Clauses (SCCs) agreement, which, in addition to containing standard data protection clauses ratified by the European Commission, sets forth the specific details of the data transfer.

The United States has no comprehensive federal privacy law and has not, at a national level, been deemed to afford data an "adequate" level of protection. In 2016, however, the European Commission issued a decision approving of the EU-U.S. Privacy Shield Framework as providing a level of protection commensurate with that provided under EU privacy law. According to the Privacy Shield Framework's website, nearly 5,400 entities have self-registered under the Framework and have likely relied on that registration to legitimize data transfers from the EU.

Overview of the *Schrems II* Decision

Shortly after Edward Snowden blew the whistle on the National Security Agency's secret surveillance programs, Austrian activist Maximillian Schrems filed a complaint with the Irish Data Protection Authority (Irish DPA) seeking to prohibit Facebook from transferring his personal data from its servers located in Ireland to its U.S. servers. As the basis for his request, Schrems claimed that U.S. data protection law does not afford EU data subjects protection comparable to what they receive under EU law—particularly when it comes to surveillance and other access by public authorities.

In opposing the suit, Facebook invoked the existence of SCCs executed by its Irish and U.S. entities. The Irish DPA sought guidance from the High Court of Ireland, which in turn asked the CJEU to issue a preliminary opinion on a number of transfer-related issues.

Although the Privacy Shield Framework, which was created after the lawsuit was filed (and to which Facebook is indeed a member),

was not itself directly challenged in Schrems' lawsuit, **the CJEU ultimately invalidated the Commission's 2016 adequacy decision on the ground that the Framework does not afford a level of protection essentially equivalent to that guaranteed by the GDPR within the EU**. The key conflict identified by the Court was not between EU and U.S. data privacy law *per se*, but rather between EU privacy law and the supremacy of U.S. *surveillance* law. Specifically, the Court highlighted that EU data subjects' information is vulnerable, both during and after transfer, to access and surveillance by U.S. governmental authorities, and noted that data subjects are left with inadequate recourse under U.S. law when their rights are infringed. In short, **the CJEU concluded that a privacy shield that does not meaningfully protect against government access to personal data is no shield at all.**

On the other hand, **the CJEU upheld the continued validity of SCCs as a data-transfer mechanism**. Notwithstanding, the Court stressed that the mere act of executing SCCs does not alone ensure GDPR compliance; rather, **both the EU-based controller and the foreign transferee are responsible for analyzing, on a case-by-case basis, whether the law of the transferee country, including the enforcement of legislation regarding public authorities' access to personal data, ensures adequate protection of that data.** If not, then the transfer should either not proceed or supplemental safeguards to ensure compliance with the GDPR-mandated level of protection must be adopted.

The *Schrems II* court also reiterated the crucial role that the national data protection authorities play in monitoring application and ensuring enforcement of the GDPR in the context of data transfers to third countries. The CJEU stressed that a DPA has the obligation to suspend or prohibit international data transfers where, "in light of all the circumstances," it finds that the requirements set forth in the SCCs cannot be complied with—particularly, where the law of the transferee country "allows its public authorities to interfere with the rights of the data subjects to which that data relates."

As the EU's top court, there is no opportunity to appeal the CJEU's decision. The case will now be returned to the Irish DPA to determine whether Facebook is able to comply, and indeed complies, with the obligations set forth in its SCCs.

What Does This Mean for U.S. Entities that Process EU Residents' Personal Data?

The entities most immediately affected by this decision are those that, until now, have relied on adherence to the Privacy Shield Framework to ensure compliance with the GDPR's restrictions on EU-U.S. data transfers. These organizations now must review each EU-U.S. data transfer and either ensure a different transfer mechanism is already in place or implement one.

For U.S. entities that rely on SCCs to transfer personal data, this opinion leaves clear that they may continue to do so, as long as they are able to ensure adequate protection of the data transferred. It is, therefore, important for organizations to revisit the SCCs they have executed to ensure—in light of *Schrems II*—that continued compliance with the obligations recited therein is feasible.

For organizations like Facebook that have previously been, or which are likely to be, subject to government surveillance or requests for access, ensuring data will receive GDPR-level protection is markedly more difficult. It is expected that the DPAs, and likely the European Data Protection Board, will issue guidance in the coming weeks and months to help organizations navigate the compliance challenges *Schrems II* creates. This guidance may also set forth certain "grace periods" to provide organizations that have relied on the Privacy Shield Framework and SCCs time to modify their approach to legal transfers to comply with the CJEU's opinion.

Shook's data privacy experts will continue to analyze the impact of the *Schrems II* decision on our clients' business activities and monitor for responses and insights from EU data protection authorities.