wiley

NEWSLETTER

Privacy Shield: On Borrowed Time? How to Prepare for Disruptions in EU-US Data Transfer Rules

February 2020

Privacy in Focus®

Businesses have limited options to transfer personal information from the European Union (EU) to the United States in compliance with the General Data Protection Regulation (GDPR). Two of the most common transfer mechanisms, Standard Contractual Clauses (SCCs) and the EU-U.S. Privacy Shield Framework (Privacy Shield), are under attack. These widely used mechanisms have been challenged in cases pending before the Court of Justice of the European Union (CJEU) as we discussed in detail here. While recent developments at the CJEU have left SCCs and Privacy Shield in play for now, the future of these transfer mechanisms is by no means secure. What will it mean for your business if they are changed or invalidated?

Overview of the Pending Challenges

SCCs have been challenged in the case *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (C-311/18) (*Schrems II*), which is currently pending before the CJEU. *Schrems II* asserts, in part, that because U.S. surveillance laws require companies to provide the U.S. government access to the personal information of individuals – regardless of citizenship – the data security protocols contained in SCCs that prohibit certain sharing practices cannot be complied with when personal information is set to the United States.

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

SCCs survived their first hurdle in this proceeding when the CJEU Advocate General (CJEU AG) issued a nonbinding decision in *Schrems II* that upheld the validity of SCCs. The court is not required to give deference to the CJEU AG's decision, however, but it frequently does so. The CJEU AG's decision wasn't without controversy as it proposed to add a further compliance layer to the use of SCCs. Specifically, the CJEU AG recommended that to rely on SCCs as a valid transfer mechanism, the business must conduct a detailed examination of each specific data transfer, including an evaluation of the parties involved in the transfer, to ensure it will comply with the terms of the SCC. The CJEU AG likewise proposed a new oversight role for Data Protection Authorities (DPAs), which would require the DPA to suspend a data transfer if it was not in compliance with the terms of the SCC.

There has been significant debate about whether the CJEU should consider the Privacy Shield in connection with *Schrems II*. The CJEU AG concluded that the CJEU should not consider the validity of the Privacy Shield in deciding this case, but then – in a blow to advocates of the Privacy Shield – dedicated 10 pages of the decision to a discussion of the program's deficiencies.

The court is not bound by the Advocate General's decision and may reach a different conclusion on the validity of SCCs, Privacy Shield, or both transfer mechanisms.

Even if the court adopts the Advocate General's position on these transfer mechanisms, the Privacy Shield is the subject of another challenge in *Quadrature du Net v. Commission*, which is expected to be argued before the CJEU later this year. In that case, French privacy groups similarly argue that, like the Safe Harbor agreement, the Privacy Shield fails to uphold fundamental EU rights and allows mass surveillance abuses by U.S authorities.

What Are Your Options to Prepare for Disruption?

Valid transfer mechanisms for personal information are crucial to transborder business. In this time of uncertainty, what can a business do to prepare for changes to or (worst case) invalidation of a transfer mechanism?

First, review your current practices and research your options. While both SCCs and Privacy Shield are being challenged, any successor mechanism is likely to be based on a similar structure. Review the currently authorized SCCs, found here. If the structure of this mechanism survives, perhaps with additional layers of scrutiny, could your company comply with the contractual terms? To implement SCCs, you must incorporate the SCCs into each contract that involves the transfer of personal information from the EU to the U.S., usually through a Data Protection Addendum. If SCCs are not an option for your business, then review the Privacy Shield framework, found here, to identify whether your business could implement this option if it survives this legal challenge.

Second, consider whether the cross-border transfer of all personal information is necessary. Could certain information be stored in the EU, reducing the amount of information subject to a transfer? Both the GDPR and many U.S. legislative proposals emphasize the importance of data minimization, which limits the collection, storage, and use of personal data to only what is necessary for carrying out the purposes for which the

information was collected. This principle does not limit the conditions of data transfer, but its growing prevalence means that companies will need to be looking more closely at whether certain data collection practices are necessary in the first place. You can get ahead of the curve by closely examining your business's current data collection and cross-border transfer practices to ensure that only personal information that is required for your stated business purpose is being collected and transferred.

Third, make sure that your actual privacy practices match your public representations. The Federal Trade Commission has settled with 16 companies in the past year that allegedly misrepresented their participation in the EU-U.S. Privacy Shield framework. A number of those involved companies that failed to re-certify on an annual basis, but continued to claim they were certified. As the privacy landscape shifts, business practices must also change to remain in compliance. Ensure that your business's internal practices remain consistent with your public statements.

Finally, consider your advocacy strategy. If the CJEU decision invalidates or compromises the effectiveness of one or both of these data mechanisms, both the US and EU will come under pressure to find additional solutions. Business should understand what industry coalitions may be involved and how to provide input on the nuts and bolts of how the CJEU decision will affect your business.

The CJEU decisions in Schrems II and Quadrature du Net may upend the data transfer environment that many businesses rely upon. Businesses that fully understand their current privacy and data governance practices and data flows will be better positioned to adapt.