akerman

Practice Update

Schrems II and EU-U.S. Personal Information Transfers: Where Are We, and What's Next?

August 4, 2020

By Elizabeth F. Hodge, S. Montaye Sigmon, and Christy S. Hawkins

The Court of Justice of the European Union (CJEU) recently issued a decision with global implications for data transfers from the EU in a case referred to the CJEU from the Irish Data Protection Commissioner, colloquially referred to as "*Schrems II*." The primary question before the CJEU was whether the transfer of an Austrian national's data from Ireland to the United States pursuant to standard data protection clauses (SCCs) was permissible in light of U.S. law and its level of protections (or lack thereof) for the personal information of EU citizens. The CJEU found that generally SCCs are valid. However, in reviewing whether an adequate level of protection exists in the United States for EU citizens, the CJEU considered, among other things, the EU-U.S. Privacy Shield framework and specifically concluded that Privacy Shield does not provide adequate protection. Therefore, the CJEU invalidated the EU-U.S. Privacy Shield as an approved mechanism to transfer personal information from the EU (or about persons located in the EU) to the United States.

Beyond the invalidation of the Privacy Shield, *Schrems II* will have an impact on companies using other mechanisms to transfer personal information to the United States. Although the CJEU affirmed the validity of SCCs, it also clarified that data exporters

Related People

Christy S. Hawkins
Elizabeth F. Hodge
S. Montaye Sigmon

Related Work

Data Privacy and Security

Related Offices

Dallas
West Palm Beach

cannot just "check the box" when using SCCs. Parties transferring personal information from the EU must verify on a case-by-case basis that the law of the country of destination ensures adequate protection, under EU law, of personal information being transferred pursuant to SCCs. Where necessary to meet the requirements of EU law, data controllers (and processors) must implement additional safeguards beyond those offered by the SCCs. Finally, if the data exporter is not able to take additional measures to safeguard the personal information of EU residents, it must suspend or end the transfer of personal information to the third country. The rationale of the CJEU in invalidating the EU-U.S. Privacy Shield, namely U.S. law regarding government surveillance, calls into question the viability of SCCs (and perhaps Binding Corporate Rules) with respect to at least some data transfers to the United States.

On July 23, 2020, the European Data Protection Board (EDPB) adopted FAQs to provide some preliminary answers regarding the scope of the CJEU's ruling, the implications of *Schrems II* on transfer tools other than the Privacy Shield, and other issues. In particular, the EDPB confirmed that whether a company can transfer personal information on the basis of SCCs "will depend on the result of [the company's] assessment, taking into account the circumstances of the transfers, and supplementary measures [the company] could put in place," (*see* Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 (adopted July 23, 2020), FAQ 5), but noted that "[t]he EDPB is looking further into what these supplementary measures could consist of and will provide more guidance." (*Id.* at FAQ 10.)

The U.S. Department of Commerce's International Trade Administration also published its own FAQs on July 31, 2020, confirming that *Schrems II* does not relieve participating companies of their obligations under the Privacy Shield. The FAQs also confirm that the U.S. Department of Commerce will

work with the European Commission and EDPB to "ensure continuity in transatlantic data flows and privacy protections." The FAQs recommend that companies seeking help in determining the most appropriate data transfer mechanism in the wake of *Schrems II* contact the European Commission, the appropriate European national data protection authority or legal counsel.

As a result of *Schrems II*, the viability of EU-U.S. data transfer mechanisms is uncertain, and there is currently no concrete guidance on exactly what companies must do to lawfully transfer personal information from the EU to the United States. Adding to the challenge is the fact that the CJEU did not provide a grace period when it invalidated the EU-U.S. Privacy Shield. However, here are three things companies should consider in the meantime to help mitigate some (but not all) of the risk from data transfers from the EU to the United States.

1. **Consider Guidance and Statements from Relevant Data Protection Authorities**

   At the highest level, the CJEU found in *Schrems II* that the Privacy Shield is not a valid data transfer mechanism because the United States does not provide an adequate level of protection of EU data subjects' personal information. Even though this finding was specifically applied to invalidate the Privacy Shield as a transfer mechanism and focused primarily on U.S. authorities' intelligence activities, many EU data protection authorities (DPAs) have already weighed in on whether continued transfers of personal information to the United States under any transfer mechanism can be made lawfully. In addition to the impact of *Schrems II* itself, the statements made by these DPAs may impact the continued viability of transfer mechanisms such as SCCs, Binding Corporate Rules, and others. Indeed, some DPAs have generally stated that SCCs are still valid, and that EU member states need to take a uniform approach to evaluating whether adequate

safeguards exist in the importer's country, while at least one DPA has opined that SCCs are as unsuitable as the Privacy Shield as a mechanism to transfer EU personal information from the EU to the United States. With EU member states issuing a wide range of statements, the level of risk a company might face may depend, at least in part, on which DPAs have authority over it. Companies should determine which jurisdictions may be relevant to them and stay informed about any statements issued by those DPAs.

2. **Re-Evaluate Privacy Programs**

   While we wait for additional guidance from the EDPB and DPAs on what kinds of supplementary measures companies will need when using SCCs to transfer personal information to third countries, at least one thing is clear: to the extent there was any doubt, regulators expect companies to comply with the data privacy obligations that apply to them, including those stemming from data transfer mechanisms. As noted above, the Federal Trade Commission has already indicated that companies certifying under Privacy Shield still have an obligation to meet the Privacy Shield requirements notwithstanding the *Schrems II* decision.

   Companies should use this as an opportunity to take a close look at what they (and any third parties with whom they share personal information) are doing to comply with all of their data privacy obligations, including those in transfer mechanisms like Privacy Shield and SCCs, and, more generally, under the General Data Protection Regulation (GDPR). The GDPR, including its Articles and Recitals, is still key when companies are evaluating their privacy practices in general. Time and resources used to evaluate, implement, and document good privacy governance and practices will be well-spent.

3. **Conduct a Risk Assessment**

The first stated objective of the GDPR is to protect data subjects' rights regarding the processing of their personal information. *See* GDPR, Art. 1. Absent a change in U.S. law, companies transferring personal information from the EU to the United States will face a certain level of risk. It follows, then, that this will require a risk-based analysis and approach. Among other things, a company's risk assessment should evaluate the kinds of personal information they are transferring from the EU and the likelihood of it being data in which U.S. governmental authorities may be interested. The higher the likelihood of interest by the government, the higher the risk to the company in connection with the transfer of the personal information to the United States. Part of the process of reconciling the *Schrems II* decision with continued transfers of personal information from the EU to the United States should necessarily involve performing and documenting risk assessments that focus specifically on the risk of transfer to EU data subjects' rights.

The future is uncertain as to whether, and if so when, companies will have the ability to rely on a clear framework that replaces the EU-U.S. Privacy Shield. What is clear from *Schrems II* is that companies should thoughtfully evaluate their data transfers out of the EU and consider any additional measures that may be needed to satisfy their obligations to safeguard personal information. Regardless of the mechanism used, companies must be wary of a "check the box" approach to personal information transfers from the EU and should tailor (and document) their approach based on the types of personal information being transferred and the purposes for which it is being transferred.

---

administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.