KRIEG DEVAULT

Insights

Unpacking Schrems II: The Demise of the EU-U.S. Privacy Shield

October 20, 2020

By: Shelley M. Jackson, Robert A. Greising, and Virginia A. Talley

On July 16, 2020, the Court of Justice of the European Union (CJEU) in Luxembourg issued its long-anticipated **decision** in the case of *Data Protection Commission v. Facebook Ireland, Schrems (Schrems II*). The decision concludes two years of litigation of a complaint initiated by Austrian privacy activist Max Schrems in May 2018, soon after the European Union's (EU) General Data Protection Regulation (GDPR) went into effect. In short, *Schrems II* (a) affirms that standard contractual clauses (SCCs) may be valid, subject to a case by case analysis, and (b) invalidates the EU-U.S. Privacy Shield framework. Organizations are digging in for the time-sensitive and difficult work of navigating EU personal data processing in a post-*Schrems II*, data-driven world.

What was the EU-U.S. Data Privacy Shield, and why did Schrems II invalidate it?

The EU-U.S. Privacy Shield was a framework aimed at providing a data transfer mechanism under which EU and U.S. companies could more easily exchange personal data in a manner compliant with EU data protection regulations. The Privacy Shield was adopted by the European Commission in 2016 in efforts to replace the International Safe Harbor Privacy Principles, which were invalidated in 2015 by *Maximillian Schrems v. Data Protection Commissioner (Schrems I)*. The Privacy Shield has since been invalidated by *Schrems II*, and as a result, over 5,000 companies that previously operated under its terms must quickly rethink their data protection strategies to once again be compliant with EU regulations.

In *Schrems II*, the CJEU held that certain government surveillance laws in the U.S. do not meet the "strictly necessary and proportional" standard required for personal data processing in the EU, and, further, do not afford data subjects with an "effective judicial remedy" to seek redress should privacy rights violations occur. As a result, *Schrems II* declared the EU-U.S. Privacy Shield framework invalid because U.S. data protection laws do not afford EU data subjects the same protections as afforded by the EU's data protection regulations

What types of data and organizations are subject to EU data protection regulations?

EU data protection regulations apply to organizations that process the personal data of EU citizens or residents, whether the organization is EU-based or not. This can include global companies that conduct trans-Atlantic data transfers on a regular basis, non-EU service providers engaged with EU businesses, and even companies that have few (if any) intentional contacts in the EU, but that nonetheless process personal data on EU data subjects. For example, non-EU companies may find themselves subject to EU data protection regulations by offering goods and services online (in a manner accessible to people in the EU) or using tools to monitor the behavior of webpage visitors (as EU data subjects may access the page). The regulations can also apply to an organization that gathers email data as part of its email marketing strategy, as the email address of an EU citizen or resident constitutes personal data protected by the GDPR.

While EU data protection regulations only apply to personal data, the term extends more broadly to include large categories of commonly collected data. The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR Art. 4 (1).

Who is impacted by *Schrems II*?

Schrems II impacts organizations that relied on the EU-U.S. Privacy Shield as a means of complying with EU data protection regulations when conducting data transfers. Certainly, those individuals whose personal data is protected by the GDPR (data subjects) and whose personal data has been or will be transferred to the U.S. are impacted by *Schrems II*. Likewise, any organization subject to the GDPR and which has transferred or seeks to transfer personal data from the EU to the U.S. or to a third country is potentially impacted.

What is the practical effect for organizations that have relied on the EU-U.S. Privacy Shield framework?

Organizations can no longer rely on the EU-U.S. Privacy Shield framework as a mechanism for lawful transfers of EU personal data to the U.S. The change mandated by *Shrems II* applies to both sending personal data and making personal data accessible to U.S. organizations, as the U.S. organizations are no longer considered compliant with EU regulations by way of the Privacy Shield. As a result, organizations must identify some other lawful basis for such transfer, including appropriate safeguards (including SCCs) pursuant to Article 46 of the GDPR, implementation of Binding Corporate Rules (often referred to as BCRs) pursuant to Article 47, or one or more exemptions (including explicit consent) pursuant to Article 49. The Department of Commerce, Department of Justice and the Office of the Director of National Intelligence have jointly released a **white paper** which explores the feasibility (from a U.S. government perspective) of post-*Schrems II* EU-U.S. data transfers using SCCs and other EU legal bases.

Does the decision impact other bases for transfer of EU personal data?

Yes. In fact, a key argument made by Mr. Schrems was that SCCs failed to ensure an adequate level of protection with respect to U.S. law. While the CJEU affirmed the validity of SCCs in theory, their ultimate effectiveness for processing of EU personal data depends on whether the SCCs provide an "adequate level of protection" as required by the GDPR. Organizations and data protection authorities therefore must examine the effectiveness of SCCs on a case-by-case basis guided by the applicable laws of the relevant jurisdictions.

If we can't use it, should we still comply with the requirements of the EU-U.S. Privacy Shield framework?

Yes. **EU-U.S. Privacy Shield certified** organizations should continue to comply with their obligations under the framework. Although *Schrems II* invalidates the effectiveness of the EU-U.S. Privacy Shield as a mechanism for EU to U.S. transfers of personal data, it does not affect a certified entity's **compliance obligations** under the EU-U.S Privacy Shield. The U.S. Department of Commerce (DOC) **announced** that participating organizations are not relieved of their Privacy Shield obligations and that the DOC will continue administering the Privacy Shield program. Further, some organizations may have contractual obligations requiring continued Privacy Shield certification and compliance.

Continued compliance also demonstrates an organization's commitment to protecting personal information, which may be beneficial as privacy regulations continue to evolve. On August 10, 2020, the U.S. Department of Commerce and the European Commission **announced** that discussions to explore an enhanced EU-U.S. Privacy Shield framework are underway.

Should an organization wish to withdraw from participation in the EU-U.S. Privacy Shield, it must follow a specific **withdrawal process**, after which certain obligations may remain in effect pertaining to data previously received under the EU-U.S. Privacy Shield. Any decision to withdraw from the EU-U.S. Privacy Shield should be made with careful consideration and with an eye toward maintaining compliance even after withdrawal.

Does this decision also invalidate the Swiss-U.S. Privacy Shield?

No. The *Schrems II* decision invalidates only the EU-U.S. Privacy Shield framework, not the Swiss-U.S. Privacy Shield framework. However, Switzerland's Federal Data Protection and Information Commissioner (FDPIC) issued a **statement** on September 8, 2020, declaring that the Swiss-U.S. Privacy Shield framework does not provide adequate protection for data transfer from Switzerland to the U.S. under Switzerland's Federal Act on Data Protection. While the FDPIC does not have the authority to invalidate the Swiss-U.S. Privacy Shield, this statement demonstrates that the Swiss-U.S. Privacy Shield may be at risk in the future. Schrems II is a cautionary tale that such frameworks are not impervious to challenge and even invalidation, so organizations should keep a close eye on future developments and should implement multiple transfer mechanisms when possible.

Is there a grace period?

Not currently, and organizations should take swift action to comply. In 2015, a similar situation occurred in *Schrems I*, and EU data protection authorities thereafter provided a brief grace period before initiating enforcement action. EU data protection authorities have yet to issue a grace period for *Schrems II*.

Next steps to consider:

- If currently EU-U.S. Privacy Shield certified, an organization should maintain basic compliance but should not continue to rely upon the framework as a mechanism for compliance with EU data protection regulations for transfers of personal data. Any decision to withdraw from EU-U.S. Privacy Shield certification should occur only in accordance with applicable compliance requirements and after exploring any contractual or other obligations to maintain EU-U.S. Privacy Shield certification.
- An organization should promptly identify all data processing activities involving international processing of EU personal data in the U.S. or in a third country and identify any compliance gaps (such as reliance on the EU-U.S. Privacy Shield) or additional obligations (such as case-by-case review of SCCs) which may have arisen due to *Schrems II*.
- An organization should consult with its Data Protection Officer, experienced privacy counsel, and/or other privacy professional to explore other grounds for EU personal data transfer and address potential compliance issues.
- An organization should continue to monitor the compliance landscape, particularly as it relates to enforcement under *Schrems II* and possible grace periods, and take additional actions as necessary.

Contact **Shelley M. Jackson**, **Robert A. Greising** or **Virginia A. Talley** of Krieg DeVault LLP with questions regarding Schrems II and its implications for your organization.