wiley

NEWSLETTER

# Schrems II Decision Upends EU-U.S. Data Transfers

July 2020

*Privacy in Focus*®

On July 16, 2020, the Court of Justice for the European Union (CJEU) issued a landmark decision in *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, Case No. C-311/18 [2020] (Grand Ct.) (Ir.) (*Schrems II*), invalidating the EU-U.S. Privacy Shield framework (Privacy Shield) as an approved data transfer mechanism, but upholding the validity of Standard Contractual Clauses (SCC) as a transfer mechanism with sufficient safeguards, with certain qualifications.

Many U.S. companies that engage in trans-Atlantic data transfers rely on either SCCs or Privacy Shield to comply with data transfer requirements under the European Union's comprehensive privacy law, the General Data Protection Regulation (GDPR). The ruling immediately disrupts the data transfer practices of businesses that rely on Privacy Shield, as the court declined to offer a grace period for transition.

**Background**

The GDPR generally prohibits cross-border transfers of data unless (1) the European Commission (Commission) has granted the recipient country an "adequacy decision," meaning the Commission has determined the country offers an adequate level of data protection;[1] (2) the controller or processor of the data provides appropriate safeguards;[2] or (3) the cross-border data transfer is justified under one of the enumerated derogations (or exceptions).[3] Cross-border data transfers were authorized under Privacy Shield, as an "adequacy decision" and SCCs as these provisions were

## Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

## Practice Areas

GDPR and Global Privacy
Privacy, Cyber & Data Governance

determined to provide appropriate safeguards.

In *Schrems II,* privacy activist Maximillian Schrems challenged the legality of SCCs used by Facebook, claiming that Europeans' data cannot be sufficiently protected in the U.S. under American surveillance laws. The case was initially brought by Schrems before the Irish Data Protection Commissioner in 2015 and transferred to the Irish courts.[4] On October 3, 2017, the Irish High Court held that U.S. surveillance under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA) had resulted in "'mass indiscriminate' processing" of Europeans' data, and SCC's provide insufficient safeguards and protections to European citizens that seek the right to redress the unauthorized processing of their data.[5]

The question before the CJEU was whether surveillance under FISA was inconsistent with European data protection laws and necessitates stronger protections for EU subjects' data than provided under SCCs.[6] Schrems' argued that SCCs provide insufficient protection for non-U.S. citizens and should be invalidated.[7] The Irish Data Protection Commissioner, argued in turn that the CJEU should also consider whether compliance with Privacy Shield was sufficient to protect EU subjects' data privacy rights.[8] On July 16, the CJEU decided both the validity of Privacy Shield and SCCs.[9]

**Privacy Shield**

Critically, in the *Schrems II* decision, the CJEU held that Privacy Shield did not provide an adequate level of protection to permit data transfers to the U.S. under Article 45 of the GDPR. Specifically, the court held that U.S. law does not provide sufficient safeguards and protections for surveillance authorized by national security statutes, including effective judicial review.[10]

In particular, the court focused on surveillance measures authorized by Section 702 of FISA and Executive Order 12333.[11] The court held that FISA Section 702 "does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes."[12] Additionally, surveillance programs based on E.O. 12333 allow access to data in transit to the United States "without that access being subject to any judicial review."[13] In light of the foregoing, the court concluded that Privacy Shield is inadequate to protect the data privacy rights of EU citizens.[14]

**Standard Contractual Clauses**

In contrast, the court upheld SCCs as a valid transfer mechanism, though not without qualifications. The court held that data transfers pursuant to SCCs are not automatically valid, but if the data controller or processor could "verify, on a case-by-case basis . . . whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses," then use of SCCs could provide the required safeguards and protections.[15]

The court noted that SCCs, by their inherently contractual nature, cannot bind the public authorities of third countries (such as the United States), but that "it may prove necessary to supplement the guarantees contained within them so that" "the level of protection of natural persons guaranteed by [GDPR Arts. 46(1) and (2)(c)] . . . is not undermined."[16] It further noted that the ability of controllers to use SCCs should not prevent them from adding other clauses or additional safeguards to supplement the protections the template clauses contain, and "depending on the prevailing position in a particular third country," supplemental measures may be *required* to ensure compliance with the level of protection mandated by EU law.[17]

Thus, the court emphasized that it is the responsibility of the controller or processor to verify, on a case by case basis, whether the law of the United States (when it is the destination country) ensures adequate protection of personal data transferred pursuant to SCCs, and provide additional safeguards where it does not.[18] In any circumstances where this cannot be achieved, the court held that controller or processor must suspend or end the transfer of EU citizen personal data to the United States.[19]

**What Happens Next for U.S. Companies?**

In its decision, the court declined to create a grace period within which the companies currently operating under Privacy Shield would be allowed to transition to an alternative data transfer mechanism. That said, individual Data Protection Authorities (DPAs) still may take a measured approach to enforcement as they did when the precursor to Privacy Shield —Safe Harbor— was invalidated, potentially providing time for companies to find alternate means to legally transfer data. The Department of Commerce (DoC) and the European Commission are also likely to engage on a potential replacement for Privacy Shield, though that will take time.

Separate from Privacy Shield, there are several other data transfer mechanisms that have been determined to provide appropriate safeguards under the GDPR, including SCCs, as well as Binding Corporate Rules (BCRs), and derogations as allowed by Article 49 of the GDPR.

SCCs: The European Commission has approved three versions of SCCs: two that cover transfers from an EU controller to a non-EU controller, and one that covers a transfer from an EU controller to a non-EU processor. The *Schrems II* decision validated the use of SCCs, although when used by a U.S.-based company, though as noted above, the use of such clauses may be subject to a case-by-case review to ensure the SCCs provide appropriate safeguards. Companies will need to closely analyze the SCCs they use and how they are implemented in light of the decision.

Derogations: The GDPR provides for certain situations when data transfers may be made even without an adequacy decision or other safeguards. The most commonly used derogations are with the explicit consent of the data subject, or when the transfer is necessary for the performance of a contract. However, the European Data Protection Board (EDPB) has cautioned that derogations are not meant to be used for routine or ongoing transfers.[20] Thus, companies will want to carefully consider the use of derogations when evaluating both short-term and long-term data transfer options.

Binding Corporate Rules: BCRs have long been the "gold-standard" of data transfer mechanisms. BCRs are created in direct consultation with a DPA. Typically, BCRs are used by large companies with wide-ranging data transfer obligations as they can take years to negotiate and involve great expense.

Finally, notwithstanding the CJEU decision, a business that has certified compliance with the Privacy Shield program is still subject to Privacy Shield obligations and enforcement in the United States. Although Privacy Shield is invalidated as a transfer mechanism by this decision, the business remains obligated –for enforcement purposes– to comply with the certifications made in its Privacy Shield registration. Indeed, in a press release issued shortly after the *Schrems II* decision, the DoC affirmed that it will continue to administer the program and "[t]oday's decision does not relieve participating organizations of their Privacy Shield obligations."[21] Thus, as businesses pivot to alternative data transfer mechanisms, they should also evaluate their obligations under the Privacy Shield program. And businesses should watch closely for updates and guidance from the U.S. government and European authorities as they put in place new data transfer mechanisms and design their data governance strategy for EU subject data.

---

[1] GDPR, Art. 45.

[2] *Id.* Art. 46.

[3] *Id.* Art. 49.

[4] Ashley Gorski, *EU Court of Justice Grapples with U.S. Surveillance in Schrems II*, Just Security (July 26, 2019), https://www.justsecurity.org/65069/eu-court-of-justice-grapples-with-u-s-surveillance-in-schrems-ii/.

[5] *Id.* (citation omitted).

[6] Jennifer Baker, *CJEU's hearing on 'Schrems II' has both sides worried ruling could be sweeping*, IAPP (July 9, 2019), https://iapp.org/news/a/cjeus-hearing-on-schrems-ii-has-both-sides-worried-ruling-could-be-sweeping/.

[7] *Id.*

[8] *Id.*

[9] In that regard, the decision departed from the non-binding opinion issued on December 12, 2019 by the CJEU Advocate General, which recommended evaluating Privacy Shield at a later date. *Id.*

[10] *Schrems II* at para. 168.

[11] Exec. Order No. 12,333, 46 Red. Red. 59941 (Dec. 4, 1981) ("E.O. 12333").

[12] *Schrems II* at para. 180.

[13] *Id.* at para. 183; *See also id.* at para. 179 where the court examined the role of the U.S. Foreign Intelligence Surveillance Court (FISC) and concluded that the supervisory role of the FISC is designed to verify whether such programs relate to the objective of collecting foreign intelligence information, not whether a given individual has or has not been properly targeted.

[14] *Id.* at para. 179.

[15] *Id.* at para. 134.

[16] *Id.* at para. 132.

[17] *Id.* at para. 133,

[18] *See id.* at para. 134.

[19] *Id.* at para. 135. The court does not single out the United States in this respect, but rather this holding applies to all third countries equally in the absence of an adequacy determination.

[20] *See* Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

[21] Press Release, DoC, U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

*Payton Alexander, a Law Clerk at Wiley, contributed to this article.*