wiley

NEWSLETTER

Companies Engaged in Trans-Atlantic Data Transfers Face Legal Uncertainty

October 2019

Privacy in Focus®

Many U.S. companies that are engaged in trans-Atlantic data transfers rely on either standard contractual clauses (SCCs) or the U.S.-EU Privacy Shield Framework to comply with data transfer requirements under the European Union's comprehensive privacy law, the General Data Protection Regulation (GDPR).[1] Recent court challenges to the "adequacy" of these data transfer mechanisms have left U.S. businesses with mounting legal uncertainty as to the future legitimacy of these long-standing data transfer practices.

Two cases before the Court of Justice of the European Union (CJEU) threaten SCCs and the Privacy Shield Framework and could require companies to develop alternative methods to comply with GDPR cross-border transfer requirements. In *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems* (C-311/18), privacy activist Maximillian Schrems – the same plaintiff whose case brought down the Safe Harbor agreement in 2015 – is challenging SCCs used by Facebook.[2] If successful, this case could compromise the viability of SCCs worldwide. In a separate case, *Quadrature du Net v. Commission* (T-738/16), three French NGOs[3] are challenging the Privacy Shield Framework, claiming that it currently violates EU fundamental rights by failing to curb surveillance abuses by the U.S. government.[4]

Privacy Shield and SCC Background

The GDPR generally prohibits cross-border transfers of data unless (1) the European Commission has granted the recipient country an "adequacy decision," meaning the Commission determined the

Authors

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

GDPR and Global Privacy
Privacy, Cyber & Data Governance

country offers an adequate level of data protection; (2) the controller or processor of the data provides appropriate safeguards; or (3) the cross-border data transfer is justified under one of the enumerated derogations.[5]

The European Union granted the U.S. a qualified adequacy decision that applies only to companies who comply with the voluntary Privacy Shield Framework.[6] The Privacy Shield Framework went into effect on August 1, 2016, replacing the 15-year-old Safe Harbor framework. The updated Framework includes stricter obligations related to data retention and cross-border transfers, more rigorous documentation and monitoring, and a prominent role for national data protection authorities in the investigation of claims.[7] Under the Privacy Shield, participating organizations self-certify to the U.S. Department of Commerce (DOC) that they will comply with the 23 privacy principles laid out in the agreement, including the principles of notice, choice, accountability, security, and data integrity.[8] Participating companies must also provide appropriate remedies for EU data subjects whose data rights have been violated under the agreement.[9] Compliance by participating companies is monitored and enforced by both the DOC and the Federal Trade Commission (FTC).[10]

While participation in the Privacy Shield Framework is increasing, the most widely used data transfer mechanism is SCCs, which are contracts entered into by senders and receivers of cross-border data that bind parties to standardized data protection clauses.[11] Companies may submit clauses to the Data Protection Authority (DPA) for approval, or choose to use the applicable model clauses that have been issued by the EU. The EU has issued three sets of model clauses for data transfers – two for transfers from EU data *controllers* to non-EU data *controllers*, and one for transfers from EU data *controllers* to non-EU data *processors*. [12]

There are other avenues for companies to bring their cross-border data practices into compliance, but most are far more costly and time-consuming than the two described above. For example, Article 46 of the GDPR allows for companies to establish Binding Corporate Rules (BCR), which serve as internal codes of conduct regulating the internal transfer of personal data between members of a corporate group. BCRs must be approved by an EU Data Protection Authority, which involves a time-consuming and expensive approval process that typically is viable only for large multinational companies.

In the absence of an adequacy decision or appropriate safeguard, cross-border data transfer may occur if a derogation, or exception, applies. The derogations listed in the GDPR are fact-specific and include situations where the data subject has explicitly consented to the data transfer or the transfer is necessary for public interest reasons, among others.[13] While derogations apply on a case-by-case basis, they alone are likely not adequate to serve as a company's primary data transfer mechanism.

Schrems II and Quadrature du Net

The legal standing of both the Privacy Shield and SCCs remain in doubt as the CJEU considers challenges to both mechanisms.

In *Facebook Ireland & Schrems,* nicknamed *Schrems II,* privacy activist Maximillian Schrems is challenging the legality of SCCs used by Facebook, claiming that Europeans' data cannot be sufficiently protected under American surveillance laws. The case was initially brought by Schrems before the Irish Data Protection Commissioner in 2015 against Facebook and transferred to the Irish courts.[14] On October 3, 2017, the Irish High Court found that U.S. surveillance acting under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA) had engaged in "mass indiscriminate processing" of Europeans' data.[15]

The question now before the CJEU is whether surveillance under FISA breaks European data protection laws and necessitates stronger protections than those provided under SCCs.[16] Schrems' argument is that Facebook is required to assist the U.S. government in surveillance of non-citizens, and thus the SCCs that facilitate this should be invalidated.[17] The Irish Data Protection Commissioner, however, believes that the Privacy Shield should also contemporaneously be considered by the CJEU, which is at odds with the European Commission's position that only SCCs should be adjudicated.[18] The eleven questions on review are expected to be decided by early 2020, with a nonbinding opinion issued on December 12, 2019 by the CJEU Advocate General.[19]

The validity of the Privacy Shield Framework will be considered by the CJEU in *Quadrature du Net v. Commission*, where French privacy groups argue that, like the Safe Harbor agreement, the Privacy Shield fails to uphold fundamental EU rights and allows mass surveillance abuses by the U.S.[20] Although the hearing was originally scheduled for July 2019, it was suspended by the CJEU until the resolution of *Schrems II*.[21] The two cases will have major implications not only for trans-Atlantic data transfers, but also the world economy.

Privacy Shield Enforcement in the U.S.

The recent challenges to the adequacy of the Privacy Shield Framework come despite increased enforcement of the Privacy Shield principles by the DOC and FTC. After the European Parliament passed a resolution in July 2018 threatening to suspend the Privacy Shield,[22] the DOC and FTC have stepped up enforcement. The DOC updated its policies and committed to increased oversight, including random web searches for false claims of compliance and quarterly "false claims reviews" to identify organizations that have not completed certification or recertification.[23]

The FTC has also committed to make enforcement of the framework a high priority, announcing a sweep of Privacy Shield actions this year.[24] The FTC requires companies participating in the Privacy Shield framework to have an "independent recourse mechanism" to resolve individual disputes and procedures for verifying compliance.[25] Where an organization fails to comply with the sanctions rulings of independent recourse mechanisms, those authorities are required to notify the FTC or the DOC.[26] The FTC may challenge the practices of participating U.S. companies under Section 5 of the Federal Trade Commission Act as "deceptive" and obtain court orders and even fines of up to $40,000 per violation.[27]

Given the recent commitment to robust enforcement of the Framework, it is critical that a business that has certified to compliance with the Privacy Shield Framework remain compliant with its requirements and closely monitor any changes to the Framework.

Looking Ahead

Given the unsettled international data transfer landscape, U.S. companies that rely on these mechanisms should keep a close eye on developments that could lead to new legal obligations. Transferring personal data to the U.S. without implementing a valid transfer mechanism can result in significant fines and penalties. In the event that the CJEU invalidates both or either of the contemporary mechanisms, companies should be prepared to revisit alternate pathways – including consent, derogations, or BCRs – to ensure GDPR-compliant data transfers.

NOTE: Stephen Conley and Kamila Benzina, who are Wiley Rein law clerks, co-authored this article with Ms. Stewart.

---

[1] A survey by the International Association of Privacy Professionals found that among 370 privacy leaders polled, 88% used standard contractual clauses last year. As of October 5, there are 4,986 organizations registered under the Privacy Shield. *See* Department of Commerce, *Privacy Shield Framework*, https://www.privacyshield.gov/list (accessed Oct. 5, 2019); Catherine Stupp, *Companies Face Uncertainty Over Challenges to Trans-Atlantic Data Transfers*, The Wall Street Journal (Sep. 23, 2019, 11:18 AM), https://www.wsj.com/articles/companies-face-uncertainty-over-challenges-to-trans-atlantic-data-transfers-11569013484?mod=searchresults&page=1&pos=2&mg=prod/com-wsj.

[2] Jennifer Baker, *EU High Court hearings to determine the future of Privacy Shield, SCCs*, IAPP (June 25, 2019), https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/.

[3] These include La Quadrature du Net, French Data Network and Fédération FDN.

[4] La Quadrature du Net, *Hearing Against the Privacy Shield Before the General Court of the EU* (May 24, 2019), https://www.laquadrature.net/en/2019/05/24/hearing-against-the-privacy-shield-before-the-general-court-of-the-eu/.

[5] Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) Article 44, 45, 46 (May 4, 2016) [hereinafter GDPR].

[6] *See* Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, Eur. Parl. Doc. P8_TA-PROV(2018)0315 (2018), http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf.

[7] *See* Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[8] Privacy Shield, *How to Join Privacy Shield*, https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 (accessed Oct. 6, 2019); Privacy Shield, *Requirements of Participation*, https://www.privacyshield.gov/article?id=Requirements-of-Participation (accessed Oct. 6, 2019).

[9] *See id.*

[10] Federal Trade Commission, *Privacy Shield*, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (accessed Oct. 6, 2019).

[11] A survey by the International Association of Privacy Professionals found that among 370 privacy leaders polled, 88% used standard contractual clauses last year. Department of Commerce, *Privacy Shield Framework*, https://www.privacyshield.gov/list (accessed Oct. 5, 2019).

[12] European Commission, *Standard Contractual Clauses (SCC),* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed Oct. 5, 2019).

[13] *See* GDPR Article 46.

[14] 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/.

[15] *Id.*

[16] 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/.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] La Quadrature du Net, *Hearing Against the Privacy Shield Before the General Court of the EU* (May 24, 2019), https://www.laquadrature.net/en/2019/05/24/hearing-against-the-privacy-shield-before-the-general-court-of-the-eu/.

[21] Baker *supra* note 30.

[22] *See generally* Privacy Shield Adequacy Resolution.

[23] *See* European Data Protection Board, *EU - U.S. Privacy Shield - Second Annual Joint Review* (Jan. 22, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf.

[24] *See* Federal Trade Commission, Privacy Shield, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield (*accessed* Oct. 7, 2019).

[25] Department of Commerce, *Enforcement of the Privacy Shield*, https://www.privacyshield.gov/article?id=Enforcement-of-Privacy-Shield (accessed Oct. 5, 2019).

[26] *Id.*

[27] *Id.*