December 30, 2019

Schrems II Advisory Opinion Endorses Standard Contractual Clauses for Cross-Border Transfer of Personal Data, But Casts Doubt on Transfers to the US and Questions Validity of Privacy Shield

On December 19, in the closely watched "Schrems II" case, Advocate General Henrik Saugmandsgaard Øe of the Court of Justice of the European Union (the "CJEU") issued an advisory opinion finding that the European Commission (the "Commission") decision authorizing the use of standard contractual clauses ("SCCs") as an adequate mechanism for cross-border transfer of personal data. In his analysis, the Advocate General highlighted the obligations of data controllers relying on SCCs to transfer data—and the authorities supervising them—to ensure that, in each case, the practices of the country where the personal data is being transferred do not undermine the rights protected by the GDPR. In this context, the Advocate General additionally raised questions concerning the validity of the Commission's "Privacy Shield" decision.

Standard Contractual Clauses

Under the EU General Data Protection Regulation (the "GDPR"), and the Charter of Fundamental Rights of the EU (the "Charter"), a data controller in the European Economic Area (the "EEA") may transfer personal data to another country outside of the EEA if the Commission has determined that the country ensures an adequate level of protection of personal data.[1] Absent such a determination, a transfer may only be made pursuant to certain safeguards detailed in the GDPR, including, inter alia, an agreement between the data controller and the receiving party under SCCs approved by the European Commission.[2] The Commission's Decision 2010/87 had established that such SCCs could be used as mechanisms for the transfer of personal data to third countries outside of the EEA.[3]

The ongoing Schrems case before the High Court of Ireland (the "High Court") challenged the validity of Decision 2010/87. The case originated in 2013, when Maximillian Schrems filed a complaint with the Irish data protection authority (the "DPA") regarding the transfer of Facebook data from EU users from servers in the EU to U.S.-based servers. Schrems alleged that, in light of the revelations made by Edward Snowden concerning the U.S government's classified global surveillance programs, the prior mechanism relied upon

1 General Data Protection Regulation, Art. 45.

2 General Data Protection Regulation, Art. 46.

3 *See Standard contractual clauses for data transfers between EU and non-EU countries*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

by U. S. companies to transfer data under the GDPR, the U.S.-EU Safe Harbor Framework ("Safe Harbor"), did not provide adequate protections for personal data. The authority initially rejected Schrems' complaint on the grounds that Commission Decision 2000/520/EC had found the protections of Safe Harbor to be adequate. In a subsequent ruling ("Schrems I"), however, the High Court rendered Decision 2000/520/EC—and, consequently, Safe Harbor—invalid, and asked the authority to reassess Schrems' complaint.[4]

In an updated complaint ("Schrems II"), Schrems challenged the new data transfer mechanism that Facebook and other companies relied upon after Safe Harbor was deemed invalid: SCCs. Schrems argued that the protections provided in SCCs were no better than those that had been provided in Safe Harbor, and that the Commission's Decision 2010/87/EU upholding their validity should be overturned. In particular, Schrems argued that the SCCs did not provide for remedies in the United States to protect the rights to respect for private life and the protection of personal data under the GDPR and the Charter.

The Advisory Opinion

The advisory opinion issued on December 19 addresses the validity of Decision 2010/87 in this context. In the opinion, the Advocate General recommends that the CJEU continue to uphold Decision 2010/87 and, therefore, continue to find SCCs to be a valid transfer mechanism under the GDPR. He begins by noting that EU law applies to "third-country" personal data transfer, even though that data might undergo processing by the public authorities in that nation. He also states that the GDPR provisions concerning data transfer are intended to ensure the continuity of a high level of protection for personal data, and that any transfer mechanisms established therein must provide protections equivalent to those provided under the GDPR itself (read in light of the Charter) in order to be valid. Therefore, in the view of the Advocate General, the SCCs adopted by Decision 2010/87/EU must ensure that level of protection in order to stand.

Next in the opinion, the Advocate General examines the validity of Decision 2010/87 in light of the GDPR and the Charter. He finds that the legitimacy of the Decision depends on the soundness of the mechanisms used to suspend or prohibit transfers. This soundness is tested whenever either a breach of the SCCs occurs, or the clauses are impossible to honor (*e.g.*, when the obligations arising under the SCCs are in conflict with laws or practices of the third country). But he finds that the mechanisms are sufficient where there exists an obligation on the part of the data controllers relying on the SCCs to suspend or prohibit such transfers in cases where the SCCs cannot be honored.

Importantly, the Advocate General emphasizes that the contractual mechanisms set out in Decision 2010/87 place responsibility on the data controller—or, failing that, on the appropriate supervisory authority—to examine the law and practices of the third party country, and to prohibit or suspend transfers

4 Case C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner* ("Schrems I").

if necessary. He explains that the "content of the examination" that parties to a data transfer agreement conduct

> entails in my view a consideration of all of the circumstances characterising each transfer, which may include the nature of the data and whether they are sensitive, the mechanisms employed by the exporter and/or the importer to ensure its security, the nature and the purpose of the processing by the public authorities of the third country which the data will undergo, the details of such processing and the limitations and safeguards ensured by that third country.[5]

The Advocate General thus concludes that Decision 2010/87/EU is not invalid because data controllers and supervisory authorities have an obligation to ensure that with respect to particular transfers, the public authorities of the third party country will not undermine the protections the transferred personal data is accorded in the EEA under the GDPR.

Privacy Shield

Separately, the Advocate General also reviewed the validity of the Commission's July 2016 "Privacy Shield" decision 2016/1250—although he urged the CJEU not to examine the validity of Privacy Shield in its decision, since it was not directly at issue in Schrems II. Under the Privacy Shield Program of the United States Department of Commerce, U.S. companies can self-certify to a framework that helps to ensure compliance with data protection requirements of the EU when personal data is transferred from the EU to the U.S.[6] In its decision 2016/1250, the Commission determined that Privacy Shield provided an adequate level of data protection to enable transfers of personal data. Thus, if a U.S. company is certified to Privacy Shield, a transfer from the EEA to that U.S. company is valid under a GDPR Article 45 adequacy determination, and no additional safeguard, such as signing SCCs, is required.

In his opinion, the Advocate General reviews Privacy Shield in light of the fundamental EU rights to respect for private life and protection of personal data, as well as the need for an effective remedy under the GDPR and the Charter. As the contractual mechanisms set out in Decision 2010/87 are inapplicable to a transfer under Privacy Shield, he questions whether there are sufficient protections in place for persons to seek judicial relief when they are subject to surveillance by the U.S. government, and concludes that there does not appear to be a sufficient mechanism in place for an individual remedy.

The Advocate General then discusses whether the ability to lodge a complaint with the Ombudsman mechanism established by the U.S. State Department as part of Privacy Shield provides a sufficient

---

5 Case C-311/18, *Data Protection Commissioner* v. *Facebook Ireland Limited, Maximillian Schrems* ("Schrems II"), Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, paragraph 135.

6 *See Privacy Shield Program Overview,* https://www.privacyshield.gov/program-overview.

alternative mechanism, and indicates that in his view, it does not. He notes that the Ombudsman mechanism is not established by law, and that the mechanism does not provide assurance that an individual will be advised if they had been a subject of surveillance, or whether any remedy has been put in place. Thus, in the Advocate General's view, the Ombudsman mechanism does not provide a "remedy before an independent body" that is able to adopt "binding reasoned decisions," and he concludes by advising that he "entertains certain doubts" about the validity of the Privacy Shield decision.

Conclusion

Although the Advocate General's opinion is not binding on the Court, the opinion may provide some additional comfort for the many organizations that have been relying on SCCs as part of the cross-border transfer of personal data, particularly where they are doing so for purposes like litigation discovery, where the data transfer is taking place with encrypted data using secure mechanisms. However, the Advocate General also makes clear that these clauses are sufficient only because data controllers and supervisory authorities retain the obligation not to transfer data where there are risks that the protections required by the GDPR will not be respected. Thus, the opinion appears to reinforce the obligations and burdens on data controllers and supervisory authorities to consider these issues with respect to each data transfer. As a result, data controllers may find themselves subject to increased scrutiny by supervisory authorities tasked with ensuring compliance with the GDPR, particularly where they are transferring data that could be the subject of surveillance by the government of a non-EU country—like the surveillance by the United States that the Advocate General finds to be problematic in his discussion of Privacy Shield.

With respect to Privacy Shield, while the Advocate General suggests the CJEU not address Privacy Shield in its opinion, he still casts doubt on its validity. The decision thus creates uncertainties for those relying on that framework as providing a valid mechanism for the cross-border transfer of personal data protected by the GDPR.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

E-Discovery Counsel Ross M. Gotler, Associate Julie L. Rooney, and Law Clerks Thomas B. Bounds and Simona Xu contributed to this Client Memorandum.