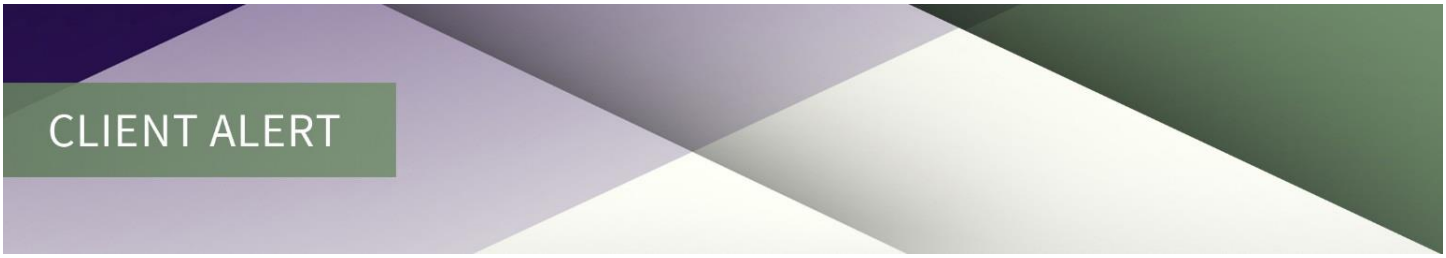

Schrems II: Some Questions Answered, More Questions Raised

July 20, 2020

AUTHORS

Daniel K. Alvarez | Richard M. Borden | Henrietta de Salis | Marilena Hyeraci
Dominique Mondoloni

On July 16, 2020, the European Union Court of Justice ("CJEU" or "Court") handed down a ground-breaking decision that casts significant doubt on the continued legality, under European Union ("EU") law, of most transfers of personal data from the EU to the United States ("U.S.").

First, the CJEU upheld adoption of the Standard Contractual Clauses ("SCCs") by the European Commission (the "Commission"). However, despite confirming the validity of SCCs as a tool for transferring data outside the EU, the Court's analysis potentially has significant implications as to both the practical utility of SCCs generally, and specifically whether SCCs can continue to be a useful mechanism in the case of transfers to the U.S. Placing the burden squarely on the shoulders of the data exporter to determine whether a third country's legal system offers adequate protections that are "essentially equivalent" to those offered in the EU creates numerous operational, legal, analytical, and logistical questions that companies must answer before they can be comfortable that the SCCs are a legitimate option in any given circumstance.

Second, the CJEU expressly invalidated the Commission's adequacy finding in the case of the EU-U.S. Privacy Shield program, finding that certain surveillance programs operated by the U.S. government unduly impinged on EU data subjects' rights and did not offer sufficient opportunities for redress, access to information, and other rights ensured by EU law.

Key Findings

This case originates in 2013, when questions were raised about the validity of the EU-U.S. Safe Harbor program in light of leaked information about U.S. government surveillance programs. That complaint led to the CJEU invalidating Safe Harbor, and the adoption by U.S. and EU officials of the Privacy Shield program. But critics argued that neither the SCCs nor Privacy Shield addressed the underlying problems presented by U.S. surveillance programs. The issue eventually made its way to the CJEU.

With respect to the SCCs, the Court decided that they remain a valid option for parties seeking to transfer personal data outside the EU, but emphasized that they impose an obligation (i) on the data exporter to verify prior to any transfer whether the level of protection in the third country is adequate, and (ii) on the data importer to inform the data exporter of an inability to comply with applicable data protection rules. Specifically, the Court said:

- While SCCs may be sufficiently protective of personal data in some circumstances, "there are others in which the context of those [SCCs] might not constitute a sufficient means of ensuring . . . the effective protection of personal data transferred to a third country," such as countries "where the law of that . . . country allows its public authorities to interfere with the rights of the data subjects to which the data relates."[1]

- Parties to the SCCs in a particular instance must look beyond the SCCs to the legal system of the recipient country to determine if the protection afforded in that circumstance is sufficient for EU law purposes.[2]

- Responsibility for making that determination lies with the data exporter: "It is therefore, above, all, for that [data exporter] to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection."[3]

- Data importers share some responsibility, in particular with respect to informing the data exporter "promptly of any inability to comply with" the SCCs, including to the extent there is any "change in national legislation" likely to change the adequacy analysis.[4]

- National regulators and the European Data Protection Board have a role to play, as well, both with respect to nullifying any SCCs that ostensibly protect data being transferred outside the EU but which are sending data to

[1] Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C‑ 311/18, ¶ 126 (July 16, 2020) ("Schrems II").

[2] "[T]he assessment of the level of protection afforded in the context of such a transfer must, in particular, take in consideration ***both*** the [SCCs]…[. . .]and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country." *Id.* ¶ 105 (emphasis added).

[3] *Id.* ¶ 134. To the extent that such issues can be cured by supplementing the SCCs, data exporters may (or are expected to) do so. *See id.* ¶ 133.

[4] *Id.* ¶ 139.

countries without sufficient protections, and with respect to identifying proactively those countries to which transfers subject to SCCs provide adequate protections.[5]

With respect to the Privacy Shield decision, the Court's focus is on whether "surveillance programs" based on Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order 12333 provide sufficient protection to EU data subjects by providing for some form of redress if they decide that their personal data has been inappropriately processed. The Court concludes that they do not.[6] Moreover, the Court readily dismisses some of the mechanisms built into the Privacy Shield as wholly insufficient, concluding that they do not ensure either sufficient independence or the existence of rules that bind U.S. intelligence services.[7]

Questions Raised, But Unanswered

While addressing the big questions regarding the validity (or not) of the SCCs and Privacy Shield, the Court's decision raises numerous questions that companies are going to have to grapple with over the coming months. For example:

- What does the Privacy Shield analysis mean for SCCs used to transfer data to the US more broadly? The Court's focus on the intelligence gathering programs that potentially implicate bulk data transfers coming into the U.S. raises questions about whether SCCs are a satisfactory mechanism for transferring data from the EU to the U.S., and who bears responsibility for making that decision. Should data exporters infer from the Privacy Shield analysis that transfers of data to the U.S. are unlikely to offer sufficient protection?

- What does this mean for transfers of personal data from the EU to the U.S. undertaken pursuant to other mechanisms, like consent or binding corporate rules? Do companies need to reconsider the notice they provide before seeking consent?

- What exactly is expected of data exporters? Is it sufficient that a data exporter secure representations from the data importer, or must it make additional inquiries or conduct additional diligence into whether the recipient country has adequate protections? Is this analysis going to be informed by considerations like the amount, sensitivity, and type of data at issue or the nature of the data importer's business?

- Equally, what must data importers do to satisfy data exporters regarding the legislative situation in the recipient country? Do data importers need to consider taking on additional liability – or moving their operations (or, at least, their cloud servers) to countries that already have an adequacy determination?

---

5 *Id.* ¶ 121.

6 For example, "Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programs for the purposes of foreign intelligence of the existence of guarantees for non-[U.S.] persons potentially targeted by those programs." *Id.* ¶ 147.

7 *Id.* ¶ 180.

- The court says that data exporters can consider *additional* contractual provisions to address any concerns about the third country's legal protections, but what kind of contractual provisions could improve the legal protections for personal data that would overcome the deficiencies that have been identified by the Court? How does an exporter confidently rely on its own contract interpretation?

- Exactly what is the role of national regulators and the European Data Protection Board? Should national regulators affirmatively seek to identify third countries that they determine to have inadequate – or adequate – protections when combined with SCCs? How would that analysis differ from a broader adequacy determination? We expect additional guidance in the coming days and weeks.

- What does this mean for transfers currently ongoing subject to either the SCCs or Privacy Shield? The effect of the decision is immediate, but how will regulators respond – will there be a grace period for companies to transfer to different mechanisms?

- What does this mean for controller-to-controller SCCs? This decision only refers to the SCCs in relation to controller-to-processor transfers. EU organizations using SCCs in relation to controller-to-controller transfers may also want to consider whether the Court's decision has any implications for such transfers.

- How does this affect transfers from the EU to other countries also engaged in surveillance? For example, the United Kingdom ("UK") and the EU are negotiating an adequacy decision to allow for transfers of data between the UK and the EU following the end of the "Brexit" transition period on 31 December 2020. The Court's decision raises the concern that the EU may not make an adequacy decision with respect to data transfers to the UK, as some member states have raised concerns regarding the UK's use of surveillance techniques, and whether the UK will seek to limit transfers of personal data from the UK to the U.S.

Next Steps

With Privacy Shield invalidated and significant questions raised about the validity of SCCs in the context of transferring data to the U.S., policymakers in both Europe and the U.S. have significant work to do to answer these questions. In the aftermath of the invalidation of Safe Harbor, policymakers on both sides moved quickly to reassure industry that a solution would be crafted to ensure continued trans-Atlantic data flows. This decision – and the current political climate – is likely to make it harder for policymakers either to make such statements credibly or to fashion a workable solution. The result for most companies is going to be significant uncertainty for the foreseeable future.

In the meantime, organizations will need to take concrete steps to understand how this decision may affect their data collection and sharing practices. They will need to review and update their data privacy impact assessments, privacy policies and security measures. Organizations that had been operating pursuant to the Privacy Shield will need to consider adopting alternative instruments to the transfer of personal data from the EU to the U.S., including whether any

technical changes must be made to the data flows to provide more protection, whether the data can be retained in the EU or moved to a third country that is already subject to an adequacy decision (e.g., Canada), and any other steps – contractual and operational – to bring themselves into compliance.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Henrietta de Salis
+44 20 3580 4710
hdesalis@willkie.com

Marilena Hyeraci
+39 02 76363 1
mhyeraci@willkie.com

Dominique Mondoloni
+33 1 53 43 4568
dmondoloni@willkie.com