Schrems 2.0: CJEU invalidates EU-US Privacy Shield and emphasizes exporter obligations when using Standard Contractual Clauses

July 16, 2020 By Paul Greaves and Wim Nauwelaerts

Executive Summary

Today, the Court of Justice of the European Union ('CJEU') handed down its long-awaited judgment in the '**Schrems 2.0**' case (*Facebook Ireland and Schrems* (Case C-311/18)), about the validity of two means of legitimizing transfers of personal data outside the EEA under the EU General Data Protection Regulation ('GDPR')[1].

In somewhat of a surprise judgment, the CJEU:

- **Invalidated the EU-US Privacy Shield[2] (the 'Privacy Shield')**, meaning that it is no longer available as a mechanism for legitimizing transfers of personal data to the US.
- **Held that the Standard Contractual Clauses ('SCCs') remain valid as a legal mechanism of transferring personal data from EEA-based controllers to recipients outside the EEA[3].** However, the CJEU issued a number of clarifications and caveats on their use. The CJEU emphasized the requirement for making case-by-case assessments on their effectiveness,

and on the obligation on the exporter of the personal data to suspend the transfer if the SCCs cannot be complied with. Failing that, the competent supervisory authorities must suspend the transfer.

Background to the Case

The Schrems 1.0 Case

The case which the CJEU decided upon today has come to be known as the 'Schrems 2.0' or 'Schrems II' case. As suggested by that name, this is not the first case involving Max Schrems – an Austrian privacy activist. Schrems first filed a complaint with the Irish Data Protection Commission ('DPC') in 2013, which focused on Facebook's transfer of his personal data to Facebook Inc. in the U.S. At the time, Facebook relied upon the 'U.S.-EU Safe Harbor framework' to legitimize the transfer. Schrems' concern was, however, that his personal data was not adequately protected from unlawful access by US state security agencies.

The resulting case has come to be known as Schrems 1.0 or Schrems I, and resulted in the CJEU invalidating the U.S.-EU Safe Harbor framework in October 2015.

The Schrems 2.0 Case

In 2015, Schrems submitted a reformulated complaint to the DPC to take account of the fact that the U.S.-EU Safe Harbor framework had been struck down. The DPC established that Facebook continues to transfer personal data to Facebook Inc., in reliance in large part on the use of SCCs.

The SCCs are another safeguard used to legitimize transfers of personal data. They are standard agreements which must be executed between the data exporter and the data importer to be effective, but cannot generally be amended. There are three different types of SCCs – adopted by a series of European Commission decisions[4] – and they are by far the most common means of legitimizing data transfers under the GDPR.

Schrems' complaint did not in fact question the validity of the SCCs as a means of legitimizing data transfers in general. He requested that the DPC suspend Facebook's transfer of personal data under the SCCs claiming that:

- The agreement that Facebook relies upon to legitimize the transfer is not consistent with the relevant SCCs adopted by the European Commission.
- The SCCs could not in any event justify the transfer of his personal data to the U.S. According to Schrems, this is because under U.S. law Facebook Inc. is required make the personal data of its users available to U.S. authorities such as the NSA and the FBI, in a manner incompatible with the Charter of Fundamental Rights of the European Union.

However, after Schrems made his complaint in 2015, the case took on broader significance:

- The DPC's investigation sought to determine (i) whether the U.S. ensures adequate protection of the personal data of citizens of the EU; and (ii) whether the SCCs offer sufficient safeguards to those citizens. The DPC brought proceedings before the Irish High Court to obtain clarification on the validity of the SCCs.
- In May 2018, the Irish High Court referred the case to the CJEU along with 11 questions, which not only bore on the validity of SCCs, but also indirectly on the validity of the Privacy Shield. The Privacy Shield was designed to replace the U.S.-EU Safe Harbor after it had been declared invalid. To benefit from the Privacy Shield, an organization had to self-certify annually that it agrees to adhere to the Privacy Shield's principles.

The verdict of the CJEU in the Schrems 2.0 Case

In today's judgment, the CJEU held that **the Privacy Shield is invalid**. In short, the view of the CJEU was that the limitations on the protection of personal data arising from the domestic law of the US on the access and use by US public authorities are not sufficiently circumscribed by the Privacy Shield. The CJEU also held that the Privacy Shield does not provide data subjects in the EU with any cause of action before a body which offers sufficient guarantees.

On the other hand, the CJEU held that **the SCCs remain valid as a legal mechanism of transferring personal data from EEA-based controllers to recipients outside the EEA.** This is on the basis that the Commission Decision adopting the SCCs (i) includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law; and (ii) establishes a mechanism under which transfers of personal data under the SCCs are suspended or prohibited in the event of the breach of the SCCs, or where it is impossible to honor the SCCs.

The CJEU pointed out, in particular, that there is an obligation on the exporter (in collaboration with the recipient of the data) to verify on a case-by-case basis whether the law of the third country ensures adequate protection of personal data transferred under the SCCs. The recipient is also under an obligation to inform the data exporter of any inability to comply with the SCCs, in which case the exporter is obliged to suspend the transfer of data and/or to terminate the contract with the importer.

The obligation to suspend or terminate the transfer therefore falls primarily to the exporter of the personal data. However, the CJEU also held that if the exporter does not do so, the competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of '*all the circumstances of that transfer*', that the SCCs are not or cannot be complied with in that third country and that the data protection required by EU law cannot be ensured by other means.

The CJEU also highlighted the possibility of implementing additional protections '*by providing, where necessary, additional safeguards to those offered by* [the SCCs]'.

Potential implications for global businesses

It is clear that – with immediate effect – the Privacy Shield can no longer be used to legitimize transfers of personal data to the U.S., and the 5378 organizations currently registered to the Privacy Shield must find alternative means of doing so. One solution mentioned by the CJEU in its judgment is reliance upon the 'derogations' provided by Article 49 GDPR. That article provides that transfers outside the EEA can be legitimized by other means such as explicit consent, contract necessity, and – in some very restricted circumstances – legitimate interests. However, regulatory guidance from the European Data Protection Board (EDPB) has construed these 'derogations' very restrictively, and so companies should approach these with caution – typically as a last resort.

Companies relying on SCCs must revisit their usage of them, and make a case-by-case assessment on whether it is appropriate to continue their use, or whether it is necessary to suspend the transfer or terminate the agreement. Exporters and importers of personal data will need to work together to conduct this assessment, and in particular exporters may look to importers – who are more familiar with the laws of the importing country – for reassurances that the

importer can comply with the obligations contained in the SCCs, and provide the required level of protection.

As part of this assessment, exporters and importers may wish to consider what additional protections they could put in place in order to limit the impact of any data protection challenges they identify. Companies should be aware, however, that there are limits to the extent to which the SCCs can be amended without undermining their 'pre-authorized' nature, which would require approval from a competent supervisory authority.

Companies should also seriously consider an alternative safeguarding mechanism for transfers out of the EEA: Binding Corporate Rules ('BCRs'). BCRs may only be used for intra-group transfers (or transfers between enterprises engaged in a joint economic activity), and must be approved by the competent supervisory authority. However, they are considered by many to be the most reliable means of legitimizing transfers of personal data under the GDPR.

Companies may also look to the upcoming revised SCCs, which are currently under development by the EU Commission. Their adoption is anticipated later this year, although it is not clear at this stage what form they will take, or how they will improve on the existing SCCs.

In the coming weeks and months, companies should look out for statements from competent supervisory authorities on their appetite (or lack thereof) for taking enforcement action against companies which are impacted by today's challenging, and somewhat unexpected judgment.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

[2] Adopted by Commission Decision 2016/1250.

[3] Adopted by Commission Decision 2010/87.

[4] Commission Decisions 2001/497/EC and 2004/915/EC (which each adopt SCCs for the transfer of personal data to controllers established in third countries) and Commission Decision 2010/87/EC (which adopts SCCs for the transfer of personal data to processors established in third countries).

About Paul Greaves

Paul Greaves is an associate in the Brussels office and a member of the Privacy & Data Security Team. Paul's privacy, information technology, and data protection practice includes a focus on compliance with the General Data Protection Regulation, ePrivacy rules, and cross-border data transfers.

[Read Bio]

About Wim Nauwelaerts

Wim Nauwelaerts is a partner in the Brussels office, leading Alston & Bird's European Privacy & Data Security Team. Wim has over 20 years of experience working with global companies on their data protection, privacy, and cybersecurity needs, including General Data Protection Regulation (GDPR) readiness, data transfer, data security and breach requirements, and compliance training.

[Read Bio]