Schrems Strikes Again: EU–US Privacy Shield Suffers Same Fate as Its Predecessor

Emma Flett
Partner, Kirkland & Ellis International LLP

Jenny Wilson
Partner, Kirkland & Ellis International LLP

Jacqueline Clover
Associate, Kirkland & Ellis International LLP

Adequate level of protection; Data protection; EU law; Privacy shield; Standard forms of contract; Transfer of personal data to third countries

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued its landmark judgment in *Schrems II*,[1] invalidating the EU–US Privacy Shield with immediate effect, while upholding the European Commission's standard contractual clauses for controller-to-processor transfers (SCCs).[2] Until now, both "adequacy" mechanisms could be relied on by organisations to transfer personal data under the GDPR[3] lawfully from the EU or the European Economic Area (EEA) to the US (as well as to other countries, in the case of the SCCs).

This article summarises, at a high level, the data transfer requirements under the GDPR, the complex chronology of events leading to this judgment, and the CJEU's reasons for its decision, and provides some practical considerations for organisations which transfer, or are looking to transfer, personal data from the EU or EEA to the US (and other third countries), in light of this ruling.

Data transfers under the GDPR

Organisations seeking to transfer personal data outside the EEA must do so in accordance with the GDPR's requirements (which largely replicate the requirements in place under the GDPR's predecessor, the Data Protection Directive).[4] These requirements are intended to prevent the safeguards which apply to the processing of personal data under the GDPR from being eroded—or even lost—where the personal data has left the EEA. Underpinning these restrictions is a basic prohibition on the transfer of personal data to a third country "which does not ensure an adequate level of protection".

Organisations may therefore only transfer personal data outside of the EEA: (1) to specific jurisdictions that are recognised by the European Commission as providing an adequate level of protection for the processing of personal data[5]; (2) using one of the data transfer mechanisms listed under art.46 of the GDPR, such as the SCCs or binding corporate rules (BCRs); or (3) where a derogation to the general prohibition on cross-border transfers under art.49 of the GDPR can be relied upon (such as obtaining the data subject's consent to the transfer of his or her personal data).

Until *Schrems II*, and pursuant to an adequacy decision adopted by the European Commission in 2016 after the invalidation the EU–US Safe Harbour framework following the CJEU's decision in *Schrems I*,[6] the US was recognised as providing an adequate level of protection for the processing of personal data, but only insofar as the US-based recipient of the personal data was certified under the Privacy Shield. Where the relevant data importer organisation had certified to the Privacy Shield, the parties to the transfer did not have to take any further steps to legitimise the transfer (such as by entering into the SCCs), or seek to rely on a derogation under art.49 of the GDPR.

The SCCs are a contractual mechanism that can be relied upon to transfer personal data outside the EEA to any jurisdiction. They were approved by the European Commission as offering adequate data privacy safeguards and, although contractual, may not be modified. Many organisations choose to rely on the SCCs to transfer personal data from the EEA to the US (and other third countries).

Case history

The decision in *Schrems II* is the latest milestone in a complex and long-running continuation of a complaint initially made in 2013 by Austrian attorney and privacy advocate, Maximillian Schrems.

Both *Schrems I* and *Schrems II* arose from complaints lodged by Mr Schrems with the Irish Data Protection Commission (DPC), in which Mr Schrems challenged the lawfulness of transfers of his personal data by Facebook in Ireland to Facebook in the US, on the ground

[1] *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (C-311/18) EU:C:2020:559.
[2] Adopted pursuant to Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries [2010] OJ L39/5. The CJEU was not asked to consider the standard contractual clauses for controller-to-controller transfers, as this data transfer mechanism was not the subject of the underlying dispute between Maximillian Schrems and Facebook Ireland Ltd.
[3] General Data Protection Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.
[4] Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
[5] A list of the European Commission's adequacy decisions can be found on the EC's website.
[6] *Schrems v Data Protection Commissioner* EU:C:2015:650; [2016] 2 C.M.L.R. 2.

that the legal system in the US did not ensure adequate protection of his personal data against US national security surveillance activities.

The DPC escalated both complaints to the Irish High Court, which in turn submitted a number of questions to the CJEU for a preliminary ruling. The questions referred to the CJEU in *Schrems II* concerned (among other things): whether the SCCs constitute sufficient safeguards as to the protection of EU citizen's personal data, or, as they lack safeguards against US Government surveillance, whether the SCCs in fact violate individuals' privacy rights under arts 7, 8 and 47 of the EU Charter of Fundamental Rights.

By calling into question, in relation to the SCCs, the compatibility of US law with art.47 of the EU Charter (which requires EU citizens be provided with an effective remedy and a fair trial in relation to transfers of their data), the questions raised by the Irish High Court also, by implication, called into question the validity of the Privacy Shield. Interestingly, the Advocate General, in his non-binding opinion in *Schrems II*, had recommended that the CJEU avoid ruling on matters regarding the Privacy Shield's validity in the context of *Schrems II*, as this question was not strictly addressed to the court. Many commentators expected the CJEU to follow suit, and in this respect, the CJEU's decision on 16 July is somewhat unexpected.

In other respects, the CJEU's decision in *Schrems II* is unsurprising, as it largely follows the rationale underpinning the invalidation of the Privacy Shield's predecessor, the Safe Harbour (and as sceptics have suggested, the Privacy Shield was largely a "repackaging" of the Safe Harbour). Both regimes were adopted following an "adequacy decision" by the European Commission (in 2000 and 2016, respectively). The 2016 adequacy decision had involved consideration of law and practice in the US relating to access by US intelligence agencies to EU personal data. It referenced explanations and assurances made by the US (including the establishment of an Ombudsperson mechanism) and concluded that the Privacy Shield proposed by the US as a replacement to the Safe Harbour, offered adequate protection for EU personal data. This decision has now been overturned by the CJEU for the reasons discussed in the next section.

Notably, as the CJEU did not consider the Swiss–US Privacy Shield in its judgment, the Swiss–US Privacy Shield is not directly impacted by the ruling and remains (at least for the time being) in effect.[7]

Privacy Shield is invalid with immediate effect

In reaching its decision in *Schrems II*, the CJEU held that the Privacy Shield was invalid, in particular, for the following reasons:

- US national security surveillance programmes are not restricted by the principle of proportionality in so far as US authorities are able to access and use the personal data transferred under the Privacy Shield for purposes which go beyond what is strictly necessary and proportionate to the purpose of national security;
- the Privacy Shield's Ombudsperson mechanism does not provide effective administrative and judicial redress for the EU data subjects concerned that is "essentially equivalent" to the legal remedies provided to EU data subjects under EU law. Regarding judicial redress options for EU data subjects, the CJEU examined US law and practice relating to individuals' actionable rights before the US courts regarding the exercise of US intelligence services' powers, and concluded that the relevant provisions "cannot ensure a level of protection essentially equivalent to that guaranteed by the EU Charter …"; and[8]
- the Privacy Shield secures the primacy of US national security laws over the fundamental rights of EU data subjects whose personal data has been imported into the US under it.

Standard contractual clauses are valid, if compliance is closely monitored

Many commentators had been concerned that the CJEU might invalidate the SCCs; however, the CJEU followed the opinion of the Attorney General in upholding their use as a data transfer mechanism, explaining:

- while the SCCs do not themselves bind government authorities in the countries to which EU personal data is transferred (as government authorities are not party to the contract), this limitation does not affect their validity, as in such case the relevant data exporters can (and should seek to) rely on additional protections (discussed below). In reaching this conclusion, the CJEU relied on statements in the GDPR (including Recital 109) which anticipate the use of "other clauses and additional safeguards"

[7] On 16 July 2020, the Swiss Federal Data Protection and Information Commissioner (FDPIC) issued the following statement on the FDPIC website (available at: *https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html* [Accessed 27 July 2020]): "The FDPIC has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland. The FDPIC will examine the judgement in detail and comment on it in due course."
[8] *Schrems II* (C-311/18) EU:C:2020:559 at [180].

in cases (such as those involving government authority access) where the SCCs cannot ensure protection;
- the SCCs require the data exporter relying on them to perform a case-by-case assessment as to whether the laws of the country of importation of the personal data provide adequate protection, as under EU laws, of the personal data to be transferred, and to determine whether to supplement the contractual safeguards provided by the SCCs with additional protections; and
- the SCCs include effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law, as they provide for: (1) the suspension or prohibition of transfers of personal data by supervisory authorities in certain circumstances (e.g. in the event of a breach of the SCCs' terms); and (2) the ability for the data exporter to terminate the SCCs where they are breached by the data importer, or where the data importer is unable to comply with them (e.g. due to the national laws applicable to the data importer, which would require it to provide EU data to intelligence services).

As regards the need for additional protections, where appropriate, the CJEU was clear that organisations may not rely unquestioningly on the SCCs to legitimise transfers of personal data outside of the EEA. Indeed, as outlined above, the decision places significant obligations on data exporters wishing to rely on the SCCs. Data exporters will now be required to carefully diligence each cross-border transfer of personal data outside of the EEA and consider whether the law and practice of the relevant third country provides an "essentially equivalent" level of protection to personal data as under EU law. If not, additional safeguards may be required to provide adequate protection of the personal data (though the CJEU did not provide specific guidance as to what these may include).

Comment

As the Privacy Shield was invalidated with immediate effect—and with no transitional period for putting in place alternative data transfer mechanisms—the decision is disruptive to businesses that rely on the Privacy Shield to transfer personal data lawfully to the US. As it is currently unclear whether a grace period for enforcement will be granted, such businesses should promptly audit their international data transfer arrangements to identify where alternative data transfer mechanisms will need to be put in place with US data recipients. The alternatives are likely to include the SCCs and, to a more limited extent, the art.49 GDPR derogations—although the European Data Protection Board (EDPB) has emphasised in its current guidance that such derogations should be interpreted restrictively as they do not provide adequate protection or appropriate safeguards for the personal data transferred.[9] BCRs may also be an alternative safeguard, although they are limited to transfers among the same group of companies, or entities with a joint economic activity, and can take time to put in place (as they require regulatory approval).

All organisations which rely, or are seeking to rely on the SCCs, to transfer personal data outside of the EEA to any jurisdiction, will now need to conduct a careful assessment as to whether the country to which personal data is sent offers adequate protection. Any assessment of the SCCs must include a consideration of the content of the SCCs, the specific circumstances of the transfer, as well as the legal regime of the country receiving the transfer, and whether additional safeguards should be adopted. If the relevant data importer cannot comply with the SCCs owing to a lack of equivalent protection under the law or practice of the relevant third country, or additional measures to safeguard the data are not available, then the data exporter will be faced with a difficult decision as to whether or not the data transfer may lawfully take place under the GDPR. The CJEU in *Schrems II* did not expand on what such additional safeguards might include, and to what extent the SCCs may be modified to include such additional safeguards but the EDPB has announced following *Schrems II* that it is looking further into what such additional measures could consist of.[10] We await further regulatory guidance from the EU and UK supervisory authorities on this issue. In the meantime, exporter organisations should also consider whether there are non-contractual and technical protections that could be applied to the transferring data (such as encryption or tokenisation), to render the data incomprehensible other than to the data exporter itself.

[9] EDPB, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679* (adopted on 25 May 2018).
[10] EDPB, "Statement on the Court of Justice of the European Union Judgment in Case C-311/18" (2020).