KIRKLAND & ELLIS

Kirkland Alert

Schrems Strikes Again: EU-US Privacy Shield Suffers Same Fate as its Predecessor

10 August 2020

On 16 July 2020, the Court of Justice of the European Union ("CJEU") issued its landmark judgment in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18) ("*Schrems II*") — invalidating the EU-US Privacy Shield with immediate effect, while upholding the European Commission's standard contractual clauses for controller-to-processor transfers ("C2P SCCs"). As the CJEU was not asked to consider the standard contractual clauses for controller-to-controller transfers ("C2C SCCs"), the judgment does not directly apply to the C2C SCCs, although the judgment has wider implications for all data transfer mechanisms under Article 46 of the General Data Protection Regulation (the "GDPR") as discussed below.

This *Kirkland Alert* summarises, at a high level, the cross-border data transfer requirements under the GDPR, and provides some practical considerations for organisations that 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 of the EEA must do so in accordance with the GDPR's requirements. 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"* equivalent to that provided to personal data under EU law.

Organisations may therefore only transfer personal data outside of the EEA: (i) to specific jurisdictions that are recognised by the European Commission as providing an adequate level of protection for the processing of personal data (prior to *Schrems II*, the US was recognized as providing adequate protection but only with respect to

transfers made under the EU-US Privacy Shield); (ii) using one of the data transfer mechanisms listed under Article 46 of the GDPR, such as the C2P SCCs and C2C SCCs ("SCCs"), which are contractual mechanisms that many organisations choose to rely on to transfer personal data from the EEA to the US and other third countries, or binding corporate rules ("BCRs"); or (iii) where a derogation to the general prohibition on cross-border transfers under Article 49 GDPR can be relied upon (such as obtaining the data subject's consent).

The decision in *Schrems II*

(a) Privacy Shield is invalid with immediate effect

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 the CJEU's decision on 6 October 2015 in *Maximillian Schrems v Data Protection Commissioner* (C-362-14) ("*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 that the legal system in the US did not ensure adequate protection of his personal data against US national security surveillance activities.

The CJEU's decision in *Schrems II* largely follows the rationale underpinning the invalidation of the Privacy Shield's predecessor, the Safe Harbour, in *Schrems I*. Both regimes were adopted following an *"adequacy decision"* by the European Commission (in 2000 and 2016, respectively).

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 personal data transferred under the Privacy Shield for purposes which go beyond what is strictly necessary and proportionate to the purpose of national security.
- 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"* under EU law.
- 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.

(b) C2P SCCs are valid, if compliance is closely monitored

Many commentators had been concerned that the CJEU might invalidate the C2P SCCs; however, the CJEU upheld their use as a data transfer mechanism, explaining that:

- While the C2P 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 data exporter can (and should seek to) rely on additional protections (discussed below).
- The C2P 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 C2P SCCs with additional protections.
- The C2P SCCs include effective mechanisms that make it possible to ensure compliance with the level of protection required by EU law, as they provide for: (a) 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 C2P SCC's terms); and (b) the ability for the data exporter to terminate the C2P 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).

What does *Schrems II* mean for your organisation?

1. Data transfers to the US

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. The European Data Protection Board ("EDPB"), in its FAQ on *Schrems II* published on 23 July 2020 ("FAQ"), confirmed that any transfers under the Privacy Shield are now illegal, and that data exporters that wish to continue transferring personal data to the US must use other data transfer mechanisms. As it is currently unclear whether a grace period for enforcement will be granted, businesses which export personal data to the US 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, although compliance must be closely monitored, as discussed below;
- to a more limited extent, the Article 49 GDPR derogations — although the EDPB has emphasised in its EDPB Guidelines 2/2018 on Derogations of Article 49 under the GDPR adopted on 25 May 2018 that such derogations should be interpreted restrictively as they do not provide adequate protection for the personal data transferred; and
- BCRs, although they are limited to transfers among the same group of companies, or entities with a joint economic activity, can take time to put in place (as they require regulatory approval) and are also subject to close monitoring for compliance. Further, an organisation's ability to rely on any existing BCRs approved by the UK Information Commissioner's Office ("UK ICO") is complicated by recent EDPB guidance. In its Information Note on BCRs adopted on 22 July 2020, the EDPB announced that any UK ICO-approved BCRs now require re-approval by a lead supervisory authority in the relevant EU Member State in order to remain valid following the end of the Brexit transition period on 31 December 2020.

2. C2P SCCs

All organisations which rely, or are seeking to rely on the C2P SCCs, to transfer personal data outside of the EEA to the US or any other jurisdiction, will now need to conduct a careful assessment as to whether the country to which personal data is sent offers adequate protection.

The CJEU's decision places significant obligations on data exporters wishing to rely on the C2P SCCs. Any assessment of the C2P SCCs must include a consideration of the content of the C2P 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 C2P SCCs due 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 C2P SCCs may be modified to include such additional safeguards, but the EDPB announced in its EDPB Statement on the CJEU Judgment in Case C-311/18 following *Schrems II* that it is looking further into what such additional measures could consist of. We await further regulatory guidance from the EU and UK supervisory authorities on this issue, and to see the impact of *Schrems II* on the new SCCs which the European Commission announced in its Communication on Two Years of Application of the GDPR on 24 June 2020 will be a *"comprehensive modernisation"* of the existing SCCs. The publication date of the new SCCs is unknown.

Notwithstanding the CJEU's decision to uphold the validity of the C2P SCCs as a viable mechanism for data transfers from the EU to third countries, the judgment also casts doubt on whether the C2P SCCs (and, by implication, the C2C SCCs) can be relied on (with additional safeguards) to transfer personal data to service providers based in the US, as the CJEU specifically found that US law and practice provide inadequate protections for EU personal data. However, until statements are made to the contrary by local data protection authorities in the EU, we expect that the SCCs will continue to provide a valid mechanism for such transfers, provided that the data exporter carries out the case-by-case assessment of each relevant transfer (as discussed above). Parties to such SCCs should also continue to closely monitor for regulatory guidance and statements made by the data protection authorities in the European countries from which personal data is being transferred to the US.

3. C2C SCCs and BCRs

Although the CJEU's ruling on the C2P SCCs does not directly apply to other data transfer mechanisms, the EDPB has clarified in its FAQ that *"in general, for third countries, the threshold set by the Court also applies to all appropriate safeguards under Article 46 GDPR used to transfer data from the EEA to any third country."* As such, data exporters are now 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, whenever the data exporter uses the C2P SCCs, C2C SCCS or BCRs. As for the consequences of *Schrems II* on transfer tools other than the SCCs and BCRs, the EDPB announced in its FAQ that these are currently under consideration.

Commentary

In practice, the assessment outlined above is likely to prove challenging for organisations that depend on uninterrupted ows of personal data between the EU and US. Pending further regulatory guidance on how to complete this assessment, data 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, or whether it is both preferable and feasible to keep the personal data solely within EU borders. As a reminder, personal data may only be transferred to third countries outside the EEA where such transfer is “necessary” to achieve the intended purpose of data processing (i.e., if a service provider can still provide a service and host the data within the EU instead of in the US, then a transfer to the US would not be strictly necessary).

Authors

Emma L. Flett

Partner / London

Jennifer F. Wilson

Partner / London

Jacqueline Clover

Associate / London

Olivia Adendorff, P.C.

Partner / Dallas / Washington, D.C.

Related Services

Practices

- Intellectual Property

- Data Security & Privacy
- Technology & IP Transactions