European Court's Judgment in Schrems II Puts EU Data Flows Between A Rock And A Hard Place

July 17, 2020

Authors
Philip Woolfson, Maury Shenk, Paul Hughes

Overview
On July 16, 2020, the Court of Justice of the European Union (the Court) decided Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18 (here) (Schrems II). The case reinforces recent Court caselaw on the limitations on international transfers of personal data from the EU, invalidates the EU-US Privacy Shield agreement, and restricts the use of EU Standard Contractual Clauses for transfers of EU personal data.

This important case threatens to disrupt the flow of data between the EU and the United States (and possibly other countries), in a manner similar to and possibly more durable than the 2015 decision in Schrems v. Data Protection Commissioner, Case C-362/14 (here) (Schrems I) that invalidated the EU-US Safe Harbor agreement. Any entity that transfers personal data from the EU to the United States should pay careful attention to the implications of the decision.

EU Data Protection Law, GDPR and International Transfers

Schrems II is the latest chapter in the conflict between:

- EU data protection rules, which govern processing of personal data of EU residents and others whose data is held by an entity with an establishment in the EU; and
- commercial exploitation of personal data, particularly by the big tech platforms, many of which are based in the United States, where data protection rules are less strict (although becoming tougher).

In the EU, the protection of personal data is a fundamental right under both the Treaty on the Functioning of the European Union and the EU Charter of Fundamental Rights. The EU General Data Protection Regulation (GDPR) creates a detailed legal framework for this fundamental right, conferring specific rights on individuals (data subjects) and imposing a number of obligations on those entities (a controller) who determine the purposes to which and the means by which personal data is processed. The GDPR has direct legal force across all 27 EU Member states and, until December 31, 2020, the UK. It also applies in Iceland, Lichtenstein and Norway which, together with the EU Member States, comprise the European Economic Area (EEA).

The GDPR is enforced by national data protection authorities (a DPA) within the EU, which can impose administrative fines for GDPR breaches of up to €20 million or 4% of annual global revenue. Individual data subjects can bring a private right of action for material or non-material damage arising from a breach of their GDPR rights; the GDPR also provides for a limited form of class action.
Specifically, the Court held that:

are contractual obligations that are not binding on the authorities of the country (a third country, the US) to which data is exported.

However, it made the use of the SCCs subject to additional safeguards, ones that may be hard to apply. The rationale for the imposition of these additional obligations is the limited nature of the protection that the SCCs provide, because they are contractual obligations that are not binding on the authorities of the country (a third country, e.g., the US) to which data is exported.

In Schrems II, the Court considered the SCCs in detail, and upheld the Commission decision adopting them. However, it made the use of the SCCs subject to additional safeguards, ones that may be hard to apply. The rationale for the imposition of these additional obligations is the limited nature of the protection that the SCCs provide, because they are contractual obligations that are not binding on the authorities of the country (a third country, e.g., the US) to which data is exported.

Specifically, the Court held that:

A controller in the EEA seeking to transfer personal data, e.g., the ‘data exporter,’ to a recipient in a third country, must first undertake a due diligence exercise, in order to verify how personal data in the third country concerned is protected in practice. Additional provisions and security safeguards may be necessary to supplement the SCCs.

The foreign recipient must inform the EU data exporter of any inability to comply with the SCCs and, if unable to adopt additional measures to ensure an adequate level of data protection, the data exporter will then be obliged to suspend the transfer of data and/or to terminate the contract with the third-country recipient.

DPAs must suspend or prohibit transfers of personal data to a third country where they consider that the SCCs are not (or are incapable of being) compiled within the recipient country, and the data being transferred cannot be protected to EU standards by other means.

The GDPR provisions at issue in Schrems II restrict transfers of personal data to countries outside the EEA that do not confer an equivalent level of protection to GDPR. In broad terms, such transfers are allowed on any of the following bases:

- The European Commission has adopted an "adequacy decision" that the third country ensures an "adequate level of data protection" – the EU-US Privacy Shield was based on such an adequacy decision, allowing transfers to US organizations that comply with Privacy Shield principles.
- The EU data controller and the foreign recipient have signed a contract including data protection clauses in a form prescribed by the Commission or adopted by a national supervisory authority and approved by the Commission – the EU Standard Contractual Clauses (SCCs) addressed in Schrems II are the most important set of such clauses.
- A group of companies has adopted 'binding corporate rules' – e.g., a commitment to secure data subject rights on an intra-group basis – and where those group rules have been approved by an EU DPA.
- Individual data subjects consent to the transfer.
- The transfer is necessary for the performance of a contract with the data subject, for reasons of public interest, the defense of legal claims or in order to protect the vital interests of the data subject.

Invalidation of EU-US Privacy Shield

The EU-US Privacy Shield was adopted in 2016 after the Court in Schrems I invalidated the similar but less detailed EU-US Safe Harbor agreement.

In Schrems II, the Court took the view that the Commission had failed to undertake a comprehensive and adequate evaluation of US surveillance laws when approving the EU-US Privacy Shield and annulled the Commission’s adequacy decision adopting it. It found that US law gives authorities, such as the National Security Agency and the FBI, sweeping powers of surveillance over non-US nationals, that there is a lack of US judicial oversight over such surveillance activities, and that there are substantial obstacles to obtaining judicial redress for EU citizens concerned about US government processing of their personal data. As a result, the Court concluded that US law did not afford EU citizens a level of protection ‘essentially equivalent’ to that guaranteed by the EU Charter of Fundamental Rights, and that this rendered the Privacy Shield incompatible with the GDPR.

It remains to be seen what specific enforcement approaches will be taken towards entities that currently use the EU-US Privacy Shield. DPAs in each EU Member State have discretion on how and when to respond. When the Safe Harbor was invalidated in 2015, there was a degree of leniency in many countries for a limited period of time. Entities that currently rely on the Privacy Shield for transfers of personal data to the United States must nevertheless promptly find a new solution. There is little prospect of adoption of a replacement of the Privacy Shield for the time being, because of the Court’s rejection of both the Safe Harbor and Privacy Shield, the practical inability of the US government to make further privacy commitments under US law, and the tense political climate between the EU and the United States.

Standard Contractual Clauses Survive, But with Limits

In Schrems II, the Court also considered the SCCs in detail, and upheld the Commission decision adopting them. However, it made the use of the SCCs subject to additional safeguards, ones that may be hard to apply. The rationale for the imposition of these additional obligations is the limited nature of the protection that the SCCs provide, because they are contractual obligations that are not binding on the authorities of the country (a third country, e.g., the US) to which data is exported.

Specifically, the Court held that:

A controller in the EEA seeking to transfer personal data, e.g., the ‘data exporter,’ to a recipient in a third country, must first undertake a due diligence exercise, in order to verify how personal data in the third country concerned is protected in practice. Additional provisions and security safeguards may be necessary to supplement the SCCs.

The foreign recipient must inform the EU data exporter of any inability to comply with the SCCs and, if unable to adopt additional measures to ensure an adequate level of data protection, the data exporter will then be obliged to suspend the transfer of data and/or to terminate the contract with the third-country recipient.

DPAs must suspend or prohibit transfers of personal data to a third country where they consider that the SCCs are not (or are incapable of being) compiled within the recipient country, and the data being transferred cannot be protected to EU standards by other means.
Given the same capacity for government surveillance in the US that led to invalidation of the Privacy Shield, this approach
throws into doubt the utility of SCCs as a lawful means of transferring personal data to the US under the GDPR. Among
other things, the Court made clear that DPAs in the EU have ultimate authority over which transfers are permissible under
the SCCs, and what further restrictions are required. This raises the possibility that entities using the SCCs to transfer
personal data from multiple EU Member States will face a patchwork of country-by-country obligations — including the
possibility that SCCs may not work at all for transfers from some Member States.

To sum up: entities now using SCCs need to tread with increased caution, keeping an eye on how Schrems II will be
interpreted by the DPAs in the EU Member States where they do business. It is likely that details of processing of personal
data (such as limiting the extent of data that are processed and transferred to the United States) and technical measures
(such as effective use of encryption to restrict government access) will help entities to continue to use the SCCs.

Consent and Necessity
The Court’s judgment did not address or undermine international transfers based on data subject consent or grounds of
necessity. However, these types of transfer have their limitations. Data subjects can withdraw any consent that may
underpin the transfers, can do so at any time and as easily as they gave it. Necessity is usually the basis for transfers that
are infrequent in nature. Nevertheless, these remain available grounds for international transfers.

Where to Process?
A further option for some data controllers may keep their processing of personal data of EU residents within the EEA or in
those third countries that have been recognized by the Commission as ensuring an adequate level of data protection — an
outcome known as ‘data localization.’ But this may be an expensive or impractical solution for companies with crucial or
centralized operations in the United States.

Brexit
The Court’s decision throws a harsh spotlight on the future of data transfers from the EEA to the UK, post-Brexit. The UK
will become a third country subject to GDPR international transfer rules after December 31, 2020. Economic operators will
need a basis for EEA transfers to the UK that is recognized as lawful under the GDPR.

The Commission will endeavor to adopt an adequacy decision by the end of 2020, provided applicable conditions are
met. These include a proposal from the Commission, an opinion from the European Data Protection Board, an approval by
EU Member States, and finally adoption of the adequacy decision by the Commission. The time available for all these
steps is far shorter than that which is usually required for an adequacy decision. It remains highly uncertain whether the
Commission will timely adopt such a decision in the context of the current, rather troubled, negotiations with the UK
regarding its future relationship with the EU generally. Schrems II will add to the process heightened scrutiny of the UK’s
approach to matters such as security and surveillance.

Between A Rock And A Hard Place?
For entities with flows of EU personal data outside the EU, options will include:

- The continued use of SCCs with closer scrutiny of recipient country data protection laws and their application in
  practice, and employing supplementary contractual provisions and protective measures, where necessary.
- The use of binding corporate rules (Schrems II did not address these).
- Obtaining explicit data subject consent after the data subject has been duly informed of the possible risks. This will
  require the identification of the countries to which the data is being transferred, the recipients and also the safeguards
  employed. This consent may also be withdrawn by the data subject, making it a potentially fragile ground for regular
data transfers outside the EEA.
- Reliance on necessity, for example in the performance of a contract with the data subject.
- Limiting data transfers to those countries whose data protection laws have been deemed adequate by a binding
  Commission decision.

For many entities, these options may be significantly less attractive than those that were available before Schrems II.
Nevertheless, unless and until an effective replacement for the Privacy Shield can be conjured up by the EU and US –
which is highly unlikely in the current political environment – these hard choices are ones that entities will need to make.
They will also need to do so having regard to the degree to which they process personal data and other constraints to
which they may be subject, for example in regulated industries.

Although the biggest online enterprises will face the closest scrutiny by DPAs and activists like Max Schrems, arguably
the worst hit could be mid-size and small companies that transfer data from the EU, as they face proportionately
larger compliance burdens. Steptoe’s team, experienced in advising on cross-border data protection compliance, can help
companies to assess and implement appropriate legal solutions to enable data flows to continue despite current
uncertainty.