SPECIAL REPORT

Schrems II:

What Does the CJEU's Decision Mean for Transfers from the EEA to the US?

Practical Guidance for Businesses

JULY 2020

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

3 Executive Summary

4 What Happened in *Schrems II*?

5 What is the Impact of *Schrems II* and Who Does This Decision Affect?

5 Who is Liable?

6 What Can Be Done in the Short Term?

8 What Needs to be Done in the Long Term?

9 Likelihood of Enforcement

11 How Can We Help

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

LAURA JEHL
PARTNER & GLOBAL HEAD, GLOBAL PRIVACY AND CYBERSECURITY PRACTICE

WASHINGTON, DC
ljehl@mwe.com
Tel +1 202 756 8930

ROMAIN PERRAY
PARTNER

PARIS
rperray@mwe.com
Tel +33 1 81 69 15 27

ASHLEY WINTON
PARTNER

LONDON
awinton@mwe.com
Tel +44 20 7577 6939

For more information about McDermott Will & Emery visit mwe.com

EXECUTIVE SUMMARY

As your organisation navigates the post-*Schrems II* landscape following the CJEU's recent decision, consider McDermott your first point of call.

We have deep experience advising global clients on compliance with the complex array of privacy and cybersecurity obligations affecting data that crosses borders or relates to foreign employees and individuals. Rooted in deep analysis following the final ruling in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*, members of McDermott's internationally recognised Global Privacy & Cybersecurity group outline practical guidance and next steps to ensure your business is prepared for what's next.

WHAT HAPPENED IN *SCHREMS II?*

The General Data Protection Regulation **(GDPR)** and its predecessor laws restrict the transfer of personal data outside the European Economic Area **(EEA)** to any country whose data protection regime is not considered adequate to protect the rights of data subjects. The aim is to ensure that EEA data subjects' GDPR rights aren't compromised when their data is sent outside the GDPR's reach; for example, when it is sent to the United States or any other jurisdiction whose privacy protections are deemed inadequate. The law contains a number of mechanisms for protecting data subjects' rights when data is transferred outside the EEA. For US transfers, the most common mechanisms have been standard contractual clauses **(SCC)** approved by the European Commission or self-certification to the EU–US Privacy Shield **(PS)**.

On 16 July 2020, the Court of Justice of the European Union **(CJEU)** issued a landmark ruling that will have significant impact on EU–US data flows reliant upon either the Privacy Shield or SCCs.

PRIVACY SHIELD

The CJEU invalidated the PS on the basis that the US legal regime governing access to personal data by national security agencies does not contain adequate limitations and safeguards. The CJEU's principal concern was that when personal data is sent to the United States, certain categories of companies (primarily telecommunications, cloud storage and internet service providers) may be required to make that data available to US law enforcement and national security authorities, such as the National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA), under certain US national security laws. This data can then be used in the context of various wide-reaching security and surveillance programmes (such as PRISM and Upstream, the programmes authorised under Section 702 of the Foreign Intelligence Surveillance Act (FISA 702) and revealed by Edward Snowden). The CJEU found that:

The Fourth Amendment to the United States Constitution does not apply to EEA citizens and thus they have no means of redress against the US government for unfair or unlawful processing under Executive Order 12.333 (EO 12.333) or FISA 702.

The appointment of the ombudsperson (as required under the PS certification) did not meet the requirements of an official tribunal under European law, therefore EEA citizens did not have an adequate judicial remedy for complaints regarding processing of their personal data.

SCCS

The CJEU held that the SCC mechanism was sufficient to protect personal data, but that a case-by-case assessment was required of the data protection standards provided in the destination jurisdiction. If, by virtue of local laws in the destination country, sufficient standards of data protection cannot be guaranteed, then the SCCs will not make the transfer safe or compliant.

This is likely to be the case for EU–US transfers as the SCCs (whose primary purpose is to ensure that GDPR standards continue to apply once personal data is transferred to the United States) only have contractual force and thus cannot bind those who are not party to the SCCs. In practice, this means that they do not restrict the ability of the NSA, FBI, CIA and others to access personal data, nor what they can do with that data under US law. SCCs, which are contractual arrangements between individual entities, are not sufficient to protect data subjects against legally permitted government surveillance.

As a result, the CJEU made clear that where SCCs cannot provide sufficient data protection guarantees, the standard clauses will need to be supplemented with additional measures (see para. 133 of the CJEU's judgment).

WHAT IS THE IMPACT OF *SCHREMS II* AND WHO DOES THIS DECISION AFFECT?

The CJEU's decision is not subject to appeal and thus will have a wide ranging impact. The ruling will affect:

All 5,384 companies who have self-certified under the PS (see the list here)	✓
EEA or US companies that rely on a US service provider (*e.g.*, cloud providers, data room providers, payroll providers, etc.) certified under the PS	✓
EEA or US companies that rely on a service provider which has engaged a US subcontractor that relies upon PS	✓
EEA or US companies that transfer to US companies that rely on SCCs or PS (*e.g.*, third parties in a cross-border M&A transaction)	✓
Companies that use SCCs anywhere in the world (although note, for the purposes of this article we are focused primarily on the transfers from the EEA to the United States)	✓
Companies that use other methods of legalising the international export of personal data, such as Binding Corporate Rules (BCRs)	✓

In essence, it will directly affect companies that self-certified under the PS, along with all companies in that supply chain that rely on PS, SCCs or BCRs.

WHO IS LIABLE?

THE DATA EXPORTER, THE DATA IMPORTER OR BOTH?

It is clear that EEA data exporters have an obligation to ensure any transfer of personal data to the United States (and to any other jurisdiction deemed "inadequate") complies with the transfer requirements in Chapter V of the GDPR. Failure to do so would amount to a breach, which could attract a regulatory fine of up to €20 million (see Article 83(5)(c) GDPR).

However, the GDPR also imposes joint and several liability on any two parties *"involved in the same processing"* (see Article 82 GDPR), which means the exporter and importer would both be jointly and severally liable for damages caused by that processing in breach of the GDPR. The extent of this liability might well depend upon whether the importer is also subject to the extra-territorial reach of the GDPR; nonetheless we recommend that both the exporter and importer consider the risks and the way any liability is allocated.

The SCCs also give data subjects third-party beneficiary rights that are enforceable against either the data exporter or the data importer. In practice, this means the data subject could bring a claim against either party for their breach of the SCCs. Although historically there has been very little evidence of these third-party rights being used in court actions, they are a very powerful weapon as breach of contract claims are easy to bring, and if brought as part of a class action of affected individuals could have serious consequences for both data exporter and importer.

WHAT CAN BE DONE IN THE SHORT TERM?

ALL COMPANIES

For all businesses with EEA–US data flows, the most immediate action is to quickly get a grip on the extent to which personal data is transferred between the EEA and the United States on the basis of the EU–US Privacy Shield. Key next steps should include:

- **International data mapping exercise.** Carry out an international data mapping exercise that includes all affiliates, service providers and other third parties. Once all US recipients have been identified, map these against the PS database available on the PS website.
- **Contract finding.** Map all of your data transfer contracts to identify which legal basis is relied on to permit that data exchange between the United States and the European Union.
- **Assessment.** There is now a requirement to undertake a "case-by-case" assessment of data transfers. In practice, however, it is likely that similar transfers between the same countries are likely to be assessed in a very similar way.
- **Remediation.** Changes may need to be made to the data transfer, in terms of what data is transferred, the technological controls and protections over it and any contractual protections that should be put in place.
- **Ongoing monitoring.** Ensure that you keep track of regulatory announcements. Consider putting reminders in your diary to review (at a minimum) announcements from the Information Commissioner's Office, the European Data Protection Board, European Data Protection Supervisor or the European Commission.
- **Compliance review.** Ensure that the above steps are kept under constant review. The market is continually evolving and the optimal steps to take will develop as an iterative process.

DATA EXPORTERS: FOR COMPANIES TRANSFERRING FROM THE EUROPEAN ECONOMIC AREA TO THE UNITED STATES

For EEA-based businesses, the most immediate action is to identify transfers that rely on the PS and look at what alternative arrangements can be put in place instead.

1. SCCs?

In the short term, it will be necessary for companies to consider whether to implement SCCs where they previously relied on PS to satisfy the GDPR. For those that already have SCCs in place, it will also be necessary to determine the extent to which your organisation is affected by the new, case-by-case assessment required by the CJEU. Consider taking the following practical steps:

- Identify where you (or your group companies) entered into SCCs either directly or by reference in another contract to transfer personal data outside of the EEA.
- Create a database of all of your organisation's SCCs. In any event, this is required for Art. 30 record-keeping under the GDPR, but will also allow you to identify the number of SCC assessments that are required.
- Although assessments must be made on a case-by-case basis, you should be able to reuse much of the assessment of local law for transfers to the United States.
- Where the SCC assessment indicates that the transfer is not adequately protected, suspend the

transfer until sufficient additional protection measures can be put in place.

- Enter into additional or modified SCCs where required and implement any appropriate additional protection measures (*e.g.*, encryption, additional minimisation, pseudonymisation, additional data subject redress/compensation, additional periodic audit).

2. SCC assessment. What will this look like?

At the very minimum, such an assessment will require the data exporter to review:

- **The data and purposes.** Where the data was obtained from, the type of data being transferred and the purposes of the transfer.
- **The technological and organisational security.** It may be the case that the risk of bulk interception can be mitigated because of the encryption used. Clearly, the system that is put in place must place the keys solely in the hands of the exporter.
- **The contractual provisions in place.** Do these include additional clauses that provide additional protection – *e.g.*, onsite/remote audit provisions or regular compliance checks?
- **The US legal system.** This should be considered as it applies to your sector; sensitive industries such as healthcare and telecommunications will need to pay particular attention to applicable law. For example, as part of the wider review it will be necessary to consider the extent to which the recipient (data importer) is an "electronic communications service provider" subject to FISA 702, or a likely target of activities conducted under EO 12.333.
- **Onward transfer and sub-processing.** Particular care should be taken where personal data can be "onward transferred" to a third party and where a sub-processor is used, as there will be supply chain risk in this further transfer. The consents for any onward transfer or use of sub-processor may need to be reviewed.

3. Can an "exception" be relied upon?

There a number of limited exceptions that can provide for a lawful transfer of personal data from the EEA to the United States. These are considered exceptions by the regulator and so should be used on a limited basis. The most relevant of these are likely to include:

- **Explicit consent.** However, valid consent is going to be practically very difficult to obtain and it can be refused or withheld at any time.
- **Performance of a contract.** However, this exception is narrow as: (i) it explicitly states that it can only be used for occasional restricted transfers and is unlikely to be a valid basis for wholesale or long-term transfer; and (ii) the transfer must be "necessary" for the performance of that contact (and this is construed narrowly).
- **It is a one-off restricted transfer and it is in your compelling legitimate interests.** However, this requires you to satisfy a number of strict conditions, including informing the relevant supervisory authority.

DATA IMPORTERS: FOR COMPANIES IN THE UNITED STATES RELYING ON PS

For those companies that had self-certified to the EU–US Privacy Shield, it will be necessary to map international data flows and onward transfers of that data to determine where new compliance efforts are required.

All group companies should review the provisions of their contracts that relate to the transfer of personal data from Europe. In reviewing these contracts:

- Consider all the possible data flows and whether you or your counterparty are now in breach of that contract.
- Determine whether the contract includes language which deals with alternatives to PS.
- Evaluate whether a breach of contract by a supplier would put you in breach of any customer or other downstream contracts.
- Consider what alternative to PS might be workable for each transfer (see above options).
- Enter into amendment agreements with each counterparty to implement the new method.
- Check that the contract implements the Article 28 Controller to Processor requirements in the GDPR.
- Consider adding additional Brexit terms if your counterparty is in the United Kingdom.

WHAT NEEDS TO BE DONE IN THE LONG TERM?

There are a number of longer-term options for personal data transfers from the EEA**:**

- **BCRs for intragroup transfers**. Although these require an involved authorisation process with the supervisory authority, once approved BCRs offer a great intragroup transfer. They are flexible and can minimise compliance costs in the long term.
- **Prepare customised version of SCCs.** These must be approved by a supervisory authority.
- **Certification mechanisms**. You can make a restricted transfer if the receiver has a certification, under a scheme approved by a supervisory authority. These have yet to get much traction (and are not available in the United Kingdom), but that is likely to change.
- **An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA.** Under this you can make a restricted transfer if the receiver has signed up to a code of conduct, which has been approved by a supervisory authority. Again these have not yet gained much traction but may do so post-*Schrems II*.
- ***Ad hoc* decisions** adopted by national data protection authorities authorising data transfers based on tailored versions of the Standard Contractual Clauses.

LIKELIHOOD OF ENFORCEMENT

The latest guidance from the European Data Protection Board (EDPB) indicates that there is no grace period. Max Schrems is already pressing the Irish data protection authority for action in relation to his case. Unfortunately we think that the usual rule will apply, which is the companies with the highest profiles will be targeted first even if their privacy practices might be superior to other companies.

Perhaps the biggest risk in the short term is the possibility of action from pro-privacy campaigners and organisations, as well as class actions from affected data subjects. There has been a dramatic growth in class actions in the European Union, particularly in the United Kingdom. For all companies still seeking to rely on the Privacy Shield, this is a clear breach of the GDPR. Data subjects do not need to show a financial loss to bring successful claims for breach of the GDPR; mere distress is sufficient, so there is a real concern that this development will be seized upon by lawyers that are in the business of bringing these sorts of claims.

HOW CAN WE HELP?

We can help in a variety of ways, from free initial advice to end-to-end projects where we can take all the steps required to de-risk your business. For companies with a large number of supplier or customer contracts we have been using AI tools to help identify which contracts need to be adjusted and can use those tools to create a heat map of risks to show which contracts require more urgent attention.

To meet the need for a new "case-by-case" assessment, we have developed standardised tools which can help that process, and can integrate them into any existing privacy platform that you may have.

We are developing a bank of supplemental contractual terms for SCCs to make the selection of appropriate additional controls easier and more cost-efficient.

Finally, we can provide counsel about defending against the risk of class actions. We have acted in the defence of one of the largest European privacy class actions to date and have good tools and techniques for effective risk mitigation.

GLOBAL KEY CONTACTS

LAURA JEHL
PARTNER & GLOBAL HEAD, GLOBAL PRIVACY AND CYBERSECURITY PRACTICE

WASHINGTON, DC
ljehl@mwe.com
Tel +1 202 756 8930

ROMAIN PERRAY
PARTNER

PARIS
rperray@mwe.com
Tel +33 1 81 69 15 27

ASHLEY WINTON
PARTNER

LONDON
awinton@mwe.com
Tel +44 20 7577 6939

McDermott
Will & Emery