TECHNOLOGY

The Ruling in Schrems II

24 July 2020

AWARDS

Ireland Law Firm of the Year 2020
Chambers Europe Awards

Ireland Law Firm of the Year 2020
IFLR Europe Awards

Structured Finance & Securitisation Deal of the Year 2020 ***(Stenn trade receivables securitisation)***
IFLR Europe Awards

Ireland M&A Legal Adviser of the Year 2019
Mergermarket European M&A Awards

Best Firm in Ireland 2019
Europe Women in Business Law Awards

Best National Firm for Women in Business Law 2019
Europe Women in Business Law Awards

Best National Firm Mentoring Programme 2019
Europe Women in Business Law Awards

Best National Firm for Minority Women Lawyers 2019
Europe Women in Business Law Awards

Ireland Law Firm of the Year 2019
Who's Who Legal

European Finance Deal of the Year 2019 ***(NTMA Green Bond Transaction)***
The Lawyer European Awards

The Court of Justice of the EU (CJEU) has provided its ruling in Schrems II:

a. confirming the validity of the European Commission controller–processor Standard Contract Clauses (SCCs), in principle; and
b. finding that the EU-US Privacy Shield, a means of transferring personal data from the EU to the US approved by the European Commission in 2016, is invalid with immediate effect, as it does not meet the standard of protection guaranteed by the GDPR.

This decision requires organisations engaged in transfers of personal data to a third country to take the following actions:

a. those that rely on Privacy Shield to transfer personal data to the US must find another mechanism to do so; and
b. organisations that use SCCs to transfer personal data to a third country must carry out an assessment prior to making a transfer under the SCCs.

In this briefing we look at the questions this decision raises for in-house legal teams and how these might be addressed.

BACKGROUND

The origins of this case, C 311/18, date back to 2013 when Maximillian Schrems, an Austrian national and Facebook user, filed a complaint with the Irish Data Protection Commissioner (DPC), requesting that Facebook Ireland be prohibited from transferring his personal data to servers owned by its parent company in the United States. His complaint was made on the ground that the law and practice in force in the US did not ensure adequate protection of his personal data held in the territory against the surveillance activities in which the public authorities were engaged.

Schrems' initial complaint led to the invalidation by the CJEU of the European Commission 'Safe Harbour' adequacy decision which, up to that time, had formed the basis of many transfers of personal data from the EU to the US. This decision was subsequently replaced by the Privacy Shield mechanism (now also invalidated).

His consequent reformulated complaint, taking into account that the personal data transfers by Facebook Ireland occurred through use of Standard Contractual Clauses, was grounded on the submission that personal data was used in the context of various US monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the European Union Charter of Fundamental Rights (Charter). He argued that this could not justify the SCCs as a mechanism for the transfer of data to the US. This complaint ultimately led to a preliminary reference by the Irish High Court to the CJEU.

HOW DID THE CJEU RESPOND TO THE QUESTIONS REFERRED TO IT?

The Irish High Court referred 11 questions to the CJEU on different aspects of the case. In summary, the key findings of the CJEU are as follows:

GDPR applies to transfers to third countries for commercial purposes, including in circumstances where personal data may also be processed for security purposes

The transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country is subject to the rules of the GDPR, "*irrespective of whether, at the time of that transfer or afterwards, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security*."

An equivalent level of protection is required to be afforded to data subjects when using SCCs as a transfer mechanism to third countries

Data subjects whose personal data are transferred to a third country pursuant to SCCs must be afforded a level of protection "*essentially equivalent*" to that guaranteed within the European Union by the GDPR, read in the light of the Charter. The court stated that requires an evaluation not just of the provisions of the contract between the transferor in the EU and the recipient in that third country, but also of aspects of the legal regime in that third country that enables access to the personal data by public authorities.

National supervisory authorities are required to act to suspend or prohibit data transfers to third countries pursuant to SCCs in certain circumstances

If the supervisory authority forms the view, in the light of all the circumstances of a transfer, that the SCCs are not or cannot be complied with in that third country and the protection of the data transferred cannot be ensured by other means, and where the controller or a processor has not itself suspended or put an end to the transfer, the supervisory authority is required to suspend or prohibit the transfer, unless there is a valid Commission adequacy decision concerning the third country.

SCCs remain valid in the light of Articles 7, 8 and 47 of the Charter

The CJEU took many factors into account, including the fact that SCCs contain an effective mechanism which ensures that the transfer to a third country of personal data pursuant to the SCC is suspended or prohibited where the recipient of the transfer does not comply with the clauses or is unable to comply with them.

The EU-US Privacy Shield (adopted by the Commission pursuant to an Adequacy Decision in 2016) is invalid.

WHY WAS THE EU-US PRIVACY SHIELD FOUND TO BE INVALID?

The Adequacy Decision underlying the EU – US Privacy Shield was made on the basis of a finding of an adequate level of protection for personal data transferred from the EU to organisations in the US under the Privacy Shield. The CJEU examined this "*finding of an adequate level of protection*" in detail.

It decided that it was "*impossible to conclude*" that the EU-US Privacy Shield could ensure a level of protection essentially equivalent to that guaranteed by the GDPR.

It also found that the Ombudsman mechanism created by the US government to provide redress for EU citizens under Privacy Shield, was inadequate, as it could neither guarantee the independence of the Ombudsman, nor could it guarantee actionable rights for data subjects "*substantially equivalent*" to those required by the GDPR.

WHAT FINDINGS WERE MADE ABOUT THE USE OF SCCS?

The CJEU concluded that SCCs remain an "*appropriate safeguard*" for international data transfers under Article 46(2) GDPR but that when using SCCs an organisation must verify "*on a case-by-case basis*" that the personal data being transferred will be adequately protected in the destination country in line with the requirements of EU law. That level of protection must be "*essentially equivalent*" to that guaranteed within the European Union by the GDPR, read in the light of the Charter.

The CJEU found that the validity of SCCs depends on the existence of effective mechanisms that, in practice, enable compliance with the level of protection required by EU law, and the fact that a breach of SCCs would result in a data transfer being suspended or prohibited.

The CJEU also addressed the situation where law enforcement makes a legally binding request for disclosure of personal data, but the data importer is prohibited by law from notifying the data exporter of this. In this situation, the data importer is permitted to not notify the data exporter of the request, but must inform the data exporter of an inability to comply with SCCs.

The CJEU noted in its decision that clause 6 of the SCCs provides that breach of SCCs will result in a right for the person concerned to receive compensation for the damage suffered. If the data exporter is aware that special categories of data could be transferred to a country that does not provide adequate protection, they must notify the data subjects beforehand, or as soon as possible afterwards. If the data importer receives a notification that the laws in the third country have changed in a manner which would affect the ability to comply with the SCCs, they must then notify the data exporter.

WHAT GUIDANCE HAS BEEN ISSUED BY SUPERVISORY AUTHORITIES AND THE COMMISSION?

The DPC, the EDPB and the EDPS have issued public statements welcoming the decision of the CJEU. In particular, the DPC has welcomed the confirmation from the CJEU that whatever mechanism is used to transfer data to a third country, the protection afforded to EU citizens in respect of that data must be "*essentially equivalent*" to that which it enjoys within the EU. Vice President Jourová also issued a statement that "*transatlantic data flows can continue, based on the broad toolbox for international transfers provided by the GDPR, for instance binding corporate rules or Standard Contractual Clauses*".

In relation to the invalidity of the EU-US Privacy-Shield, the European Commission has confirmed that it is in discussions with its counterparts in the US in order to come to a shared understanding of the CJEU judgment and explore possible ways in which to address the concerns raised by the court.

The EDPB and DPC have stated that they are assessing the judgment in more detail and intend to provide further clarification for stakeholders and practical guidance on the mechanisms of transfer of personal data from the EU to third countries pursuant to the judgment.

WHAT ARE THE NEXT STEPS?

Is there a grace period?

It is hoped that data protection authorities will take a gradual approach to enforcement of Schrems II. When the Safe Harbor was struck down in 2015, data protection authorities indicated they would not take active enforcement for a few months and a similar approach now would help organisations to roll out their initial response to Schrems II.

While waiting for regulatory guidance from the EDPB and DPC, organisations might use this period to assess their transfer mechanisms. Those that have limited alternatives to reliance on the SCCs for transfers of personal data to the US might seek to put in place an assessment framework complimented by additional measures and supplemental

protections such as those we outline below.

Use of Privacy Shield

The CJEU has invalidated the EU-US Privacy Shield with immediate effect. This means that organisations solely relying on the Privacy Shield as a mechanism to transfer personal data to organisations in the US will need to promptly arrange suitable alternative mechanisms under the GDPR.

Use of SCCs

When using SCCs an organisation must verify "*on a case-by-case basis*" that the personal data being transferred will be adequately protected in the destination country in line with the requirements of EU law. The assessment of whether a third country offers adequate protection is primarily the responsibility of the exporter and the importer of the data when considering whether to enter into SCCs.

They must take into consideration the content of the SCCs, the specific circumstances of the transfer, as well as the legal regime applicable in the importer's country (in light of the non-exhaustive factors set out under Article 45(2) GDPR).

While we understand that the EDPB and the DPC are working on regulatory guidance in light of Schrems II, no such guidance exists at present. We recommend that organisations carry out that assessment now to ensure compliance with the ongoing obligations of controllers and recipients under the SCCs. Such assessment measures could include:

1. Map and assess all flows of personal data to third countries.

   Where personal data is transferred under SCCs: (i) determine the destination countries; and (ii) assess the nature of the transferring personal data, in particular:

   a. identify what personal data is being transferred;

   b. the sensitivity of this personal data; and

   c. whether some or all of this personal data is already in the public domain.

2. Determine if the destination country provides an satisfactory level of protection.

   Organisations may consider creating a risk questionnaire for completion by data importers to help to assess the third country's surveillance laws.

3. Consider additional measures and safeguards to address any risks identified.

4. Document findings and decisions made.

Use of BCRs

Organisations should also give some consideration to the adoption of BCRs as an alternative framework for compliant intra-group global data transfers. The rigorous BCR approval process, combined with the protections included within BCRs to regarding access by foreign law enforcement agencies, suggest BCRs have an important role to play in future international data transfers.

Schrems litigation:

The case will now return to the Irish High Court. As confirmed by the CJEU, the decision as to whether to prohibit or suspend the transfers from the EU to the US pursuant to the SCCs, can be taken by the DPC. It remains to be seen whether the DPC will avail of the option, referred to by the CJEU in its decision, to refer the matter to the EDPB for an opinion, or a binding decision, in order to avoid divergent decisions between national supervisory authorities.

KEY CONTACTS

Rob Corbet
Partner, Head of Technology
+353 1 920 1211
rob.corbet@arthurcox.com

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Olivia Mullooly
Partner
+353 1 920 1060
rachel.benson@arthurcox.com

Rachel Benson
Professional Support Lawyer
+353 1 920 1435
rachel.benson@arthurcox.com