LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Schrems II: Validity of SCCs referred to the CJEU

by **Peter Bolger**

Schrems II: Validity of SCCs referred to the CJEU

1st December 2017 | by Peter Bolger

In the latest case involving data privacy activist Maximillian Schrems and Facebook Ireland, on 3 October 2017 the Irish High Court decided to refer the validity of standard contractual clauses ('SCCs') for a preliminary ruling to the Court of Justice of the European Union ('CJEU').

The case concerns the transfer of personal data from Facebook Ireland Limited to its parent company in the US, Facebook Inc., and raises issues as to whether a basis for doing so used by Facebook, namely the use of SCCs, were lawful under Irish and EU data protection law. Peter Bolger, Partner and Head of IP, Technology and Privacy at LK Shields Solicitors, analyses here the background to the case and the Irish High Court's decision.

Background

Following the disclosures made by Edward Snowden about US surveillance programmes such as PRISM in June 2013, Mr Schrems originally made a complaint to the Irish Data Protection Commissioner ('IDPC') on 25 June 2013 that his personal data transferred by Facebook Ireland to the US was being unlawfully accessed by US state security agencies. Those data transfers were carried out under the Safe Harbour Decision. The IDPC declined to investigate the complaint as it was of the view it was bound to accept the Safe Harbour Decision as binding. This decision was judicially reviewed and on 18 June 2014 the Irish High Court decided to ask the CJEU to determine whether in light of Articles 7, 8 and 47 of the EU Charter of Fundamental Rights ('Charter') the IDPC was bound absolutely by the Safe Harbour Decision.

Safe Harbour struck down

The CJEU decided on 6 October 2015 that data protection authorities could and should consider complaints 'with all due diligence' and in circumstances where a data protection authority considers the complaint as well founded, the data protection authority must be able to engage in legal proceedings. Further, the CJEU ruled that the Safe Harbour Decision was invalid.

Investigation of the complaint and the proceedings

Mr Schrems' complaint was remitted back to the IDPC for investigation and was ultimately reformulated, essentially focussing on the SCCs decisions (in particular decision 2010/87/EU) rather than the Safe Harbour Decision. The IDPC then largely followed the directions at paragraph 65 of the CJEU Safe Harbour judgment.

The IDPC issued a draft decision to the parties on 24 May 2016 provisionally finding that Mr Schrems' complaint was well founded, namely there is an absence of an effective remedy in US law compatible with Article 47 of the Charter for an EU citizen whose data is transferred to the US where it may be at risk of being accessed and processed by

US state agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter. Observing that a notice prohibiting or suspending transfers did not provide an answer to the

complaint, and that neither the IDPC nor the Irish courts could determine the validity of the SCCs decisions, the IDPC commenced legal proceedings in the Irish High Court.

In essence, the question for the Irish High Court was whether to refer the validity of the SCCs to the CJEU or not, at least insofar as they involve data transfers to the US.

Amici curiae

Recognising that the outcome of the proceedings had potentially significant economic and commercial consequences, the High Court granted a number of other parties permission to participate in the proceedings as amici curiae (or 'friends of the court'). These included the United States of America and the Business Software Alliance.

Privacy versus national security

It is worth noting the High Court seemed, in a case involving close scrutiny of certain US laws, to have been at pains to make clear that it was not its function to assess or resolve the relative merits of balancing the right to privacy and national security.

The High Court considered as well-founded arguments that the laws and practices of the US do not respect the essence of the right to an effective remedy before an independent tribunal as guaranteed by Article 47 of the EU Charter of Fundamental Rights.

Substantive arguments before the Irish High Court

Are EU law and the Charter engaged?

Yes. The High Court rejected the argument that, based inter alia on Article 4(2) of the Treaty on the Functioning of the European Union ('TFEU') and Article 3(2) of Directive 95/46/EC ('Directive'), as the case concerned national security it therefore fell outside the scope of EU law. The High Court considered Article 4(2) of TFEU as applying only between the EU and Member States and that the argument ran contrary to the first Schrems decision, the views of the Article 29 Working Party (Working Document 5 December 2014) and the Commission under the Privacy Shield Decision, and further, the case here involved transfers of data between two private companies. In effect, to follow this argument would "entirely hollow out EU data protection law."

Does the Privacy Shield Decision preclude a CJEU reference?

No. The High Court rejected the view that the Privacy Shield Decision constitutes an adequacy decision in respect of the United States. It confirmed that the Privacy Shield Decision is not a decision that the US affords adequate protection of personal data transferred from the Union to the US in all circumstances and contrasted it with the comprehensive Article 25(2) adequacy decision in respect of Israel (Com. Decision 2011/6/EU (C(2011) 332).

Was the High Court restricted to only considering matters raised in the IDPC draft Decision?

No. As the High Court said, as a matter of principle it was not only entitled, but was obliged, to consider all of the facts and law properly presented to it and to decide on the basis of those facts and arguments whether or not a reference was required. In fact, there was no requirement for the IDPC to prepare a draft decision.

What is the correct comparator: Union or Member State law?

The High Court preferred the view that the adequacy of the laws of the third country should be assessed by

reference to Union law and not by reference to the laws of individual Member States. However, the Court concluded that it is a matter on which the CJEU is required to give a ruling in order to properly give effect to Union law.

The standard of EU data protection, the SCCs and the laws of third countries

The High Court then considered data transfers under Article 26 and the extent of the protection of personal data required by the Directive, and undertook a detailed analysis of SCC Decision 2010/87. The Court took the view that Article 26 is a derogation from Article 25 and that data transfers pursuant to Article 26 are not premised upon the existence of an adequate level of protection in the third country. However, the data is still entitled to a high level of protection. Therefore, the Court said, transfers of personal data to a third country cannot simply step outside the protections afforded by the Directive. Further, data exported cannot rely solely upon the SCCs as complying with the requirements of the Directive regardless of the legal regime in the third country to which the data is exported. Data protection authorities still have an obligation to ensure that the data receives a high level of protection.

Therefore, the Court held, if there are inadequacies in US law within the meaning of Union law, the SCCs cannot and do not remedy or compensate for these inadequacies.

The relevant laws of the United States

The High Court then analysed in some detail the legal basis for electronic surveillance by the United States, PRISM and Upstream; relevant data protection law in the US; the Fourth Amendment; individual remedies available to EU citizens under US law and the principle of 'standing' to bring suit in the US. The Court concluded that despite the number of possible causes of action, it could not be said that US law provides the right of every person to a judicial remedy for any breach of data privacy by US intelligence agencies. The Court accepted there are extensive rules to ensure that data is obtained in accordance with the law and, once obtained, is not misused. However, this is not the same as providing a remedy when the rules are broken and the data is unlawfully collected or otherwise misused.

Is Article 47 of the Charter engaged?

Yes. In the first Schrems decision, it was accepted by the CJEU that Article 47 applies even if the interference with data protection arose by surveillance in the US.

Do the laws of the US respect the essence of Article 47?

The High Court considered as wellfounded arguments that the laws and practices of the US do not respect the essence of the right to an effective remedy before an independent tribunal as guaranteed by Article 47 of the Charter.

Is this conclusion affected by the Ombudsperson mechanism?

Even though the High Court was satisfied that an EU citizen who reasonably believes their data was transferred to the US under the SCCs can make a request to the Ombudsperson, the High Court found there is a well founded argument that the Ombudsperson mechanism does not respect the essence of that right.

Was the IDPC correct not to suspend or prohibit the transfers?

In the final substantive point, the High Court considered that the right of the IDPC to block transfers under Article 4 of the SCC decisions does not in itself save the SCCs and that not exercising the right to block transfers in this case was a legitimate conclusion, and one for it to make as an independent supervisory authority.

Conclusion

The High Court essentially found that it agreed with the well founded concerns raised by the IDPC and that nothing had materially changed the position since the original complaint was made.
While the questions to be posed to the CJEU are not yet known, we do know that like the Safe Harbour Decision before, the CJEU will pronounce on the validity of the SCCs. This case also likely raises issues with third countries other than the US with obvious potential issues for the UK post-Brexit.

For more information please contact Peter Bolger at pbolger@lkshields.ie

This article was published in Digital Business Lawyer.

About the Author

Peter Bolger
Partner

Peter is Head of our highly regarded Intellectual Property, Technology and Privacy team. He advises clients on all aspects of privacy law in respect of compliance, registration, international transfers, policies and audits including the GDPR.
T: +353 1 638 5877 **E:** pbolger@lkshields.ie