THE BROKEN SHIELD: TOP EU COURT RESTRICTS EU-US DATA TRANSFERS

JULY 2020

By Barry Fishley and George Mole

In a landmark decision on 16th July, the European Court of Justice ("**ECJ**"), the EU's highest court, has ruled that transfers of personal data from the EU to the US using the Privacy Shield mechanism are invalid. The ECJ also confirmed that while in principle the use of the EU's standard contractual clauses ("**SCCs**"), also known as the 'Model Clauses', remains valid, supervisory authorities have an obligation to suspend or prohibit transfers of personal data to third countries (such as the US) where the laws of that country make it impossible to provide the privacy protections that the mechanism is supposed to ensure.

What are the facts of the case?

Max Schrems is an Austrian lawyer and privacy activist who won a case in 2015 ("**Schrems I**") which overturned the EU's decision to approve the use of the Safe Harbour regime to transfer personal data from the EU to the US. Mr Schrems brought the complaint in light of the allegations by Edward Snowden concerning the alleged use of mass surveillance techniques which, Mr Schrems argued, compromised the privacy of EU individuals.

In response to the decision in *Schrems I*, the US and EU Commission agreed an alternative framework for permitting the lawful transfer of personal data from the EU to the US, known as Privacy Shield. The Privacy Shield was approved by the EU Commission in July 2016 and that approval is the subject of this case, the second brought by Mr. Schrems ("**Schrems II**"). The case was heard first by the Irish High Court which referred the case to the ECJ.

At the same time as the US and EU Commission were ironing out the Privacy Shield framework, Mr Schrems made a further complaint relating to the use of SCCs. Essentially, he argued that SCCs did not properly protect EU citizens' data in the US because of the alleged potential illegal mass surveillance of EU citizens data by US authorities.

What did the case decide?

The case decided two key issues: first that the EU's decision to approve Privacy Shield for transfers of personal data from the EU to the US was invalid.

Secondly, that in principle the use of SCCs for transfers of personal data from the EU to the US remains valid. However, the ECJ made it clear that competent supervisory authorities are under an obligation to suspend or prohibit transfers of personal data to third countries (such as the US) where the laws of that country make it impossible to provide the privacy protections that the SCCs are required to provide under EU privacy laws. Accordingly, users of SCCs will need to decide whether additional safeguards protecting EU citizens' data are necessary.

What is the impact of the *Schrems II* decision?

The *Schrems II* decision is of the utmost significance for the 5,300+ organisations which are currently relying on Privacy Shield[1] as their method for transferring personal data from the EU to the US. These organisations will need to immediately consider and implement alternative legal mechanisms to ensure that such EU-US transfers of personal data are lawful.

In terms of the decision's impact on the SCCs, the extent to which supervisory authorities will examine the validity of SCCs on a case-by-case basis is, of course, unknown at this stage. However, our assessment is that in the absence of complaint from a data subject (for example a disgruntled ex-employee or customer), it is generally unlikely that supervisory authorities will proactively seek to unpick arrangements between organisations using SCCs.

The UK's ICO has said it is considering the judgment. The US government said it is doing the same and that it will continue to administer the Privacy Shield and that participating organisations are not relieved of their Privacy Shield obligations.

How can organisations lawfully transfer personal data from the EU to the US if they can no longer rely on Privacy Shield?

Organisations that are relying on Privacy Shield to transfer personal data from the EU to the US will need to put in place alternative legal arrangements to ensure such transfers are lawful.

In the first instance, organisations may want to put in place SCCs to ensure that EU-US transfers of personal data are lawful. Although the use of SCCs is open to being challenged by a supervisory authority, on a case-by-case basis, this is the simplest and quickest mechanism to ensure EU-US transfers of personal data between organisations in the short term.

1 https://www.privacyshield.gov/list

THE BROKEN SHIELD: TOP EU COURT RESTRICTS EU-US DATA TRANSFERS

JULY 2020

Organisations currently relying on Privacy Shield for EU-US transfers of personal data will need to immediately consider and put in place alternative(s)

EU Commission to update SCCs

It should be noted that the EU Commission confirmed last month that the SCCs are undergoing a "comprehensive modernisation" in light of the new requirements set out in the GDPR and that this exercise of modernisation will reflect the concerns made by the ECJ in recent case law, including *Schrems II*.[2] However, it remains unclear when such update will be approved for use and therefore, until then, organisations should use the existing SCCs.

For international personal data transfers between group entities, a mechanism which offers greater legal stability is the implementation of binding corporate rules ("**BCRs**") which, as the name suggests, binds group entities to practices that align with the requirements of EU privacy laws. However, BCRs are complex, costly and time-consuming to implement. This is because they require approval from a number of competent supervisory authorities, which can take a number of months.

In any event, organisations may not need to rely on SCCs or BCRs if they obtain explicit consent from data subjects to transfer their personal data from the EU to the US. To do so, organisations will need to make sure that the consent meets the strict consent requirements of the GDPR i.e. that the consent to transfer the personal data (and process it in the US) is specific, informed, unambiguous and affirmed in a clear statement from the data subject (preferably in writing). That said, it is unlikely that any purported consent from a data subject in the context of an employer-employee relationship will be considered valid. Accordingly, if organisations need to transfer employee personal data from the EU to the US, they should rely on the SCCs or BCRs.

What wider commercial impact will the decision have for organisations?

***IT Vendor Arrangements*:** The decision will also have an impact on any organisation that has in place arrangements with US-based IT vendors which rely on Privacy Shield and which require the vendor to handle personal data e.g. data hosting. It would be best practice for organisations to notify such IT vendors of the impact of the *Schrems II* decision and ask them to enter into SCCs to ensure that they may continue to carry out the processing of that personal data lawfully. It is likely that some of the larger, more sophisticated IT vendors will also be seeking to contact their customers on this.

***Privacy Policies*:** Organisations will also need to update their privacy notices to ensure that any change to the organisation's use of personal data (including the legal mechanism relied upon to transfer it from the EU to the US) are reflected and up to date. If organisations fail to update their privacy notices, they will be in breach of their transparency obligation under the GDPR (Article 5).

***M&A - Due Diligence*:** In the context of M&A, the legal mechanism for transferring personal data from the EU to the US will become a key diligence item. In particular, the buyer's advisors will want to know that some other lawful mechanism is in use and that the target's privacy notices have been updated to reflect any change in legal mechanism used. The buyer may also ask for specific warranties to cover this issue.

Key takeaways

- Organisations can no longer rely on the Privacy Shield framework to transfer personal data from the EU to the US, lawfully.
- Organisations currently relying on Privacy Shield for EU-US transfers of personal data will need to immediately consider and put in place alternative(s), for example SCCs, BCRs and/or rely on derogations such as explicit consent, necessary for contractual performance (for occasional transfers) and/or others set out in Article 49 of the GDPR.
- For organisations that use US-based IT vendors which rely on the Privacy Shield to process personal data in the US, it would be best practice to actively notify such vendors of the impact of the decision and ask them to enter into SCCs.
- In the M&A context, the legal mechanism(s) for EU-US transfers of personal data will become a key diligence item that may prompt the buyer to seek additional contractual protections from the seller.

2 European Commission, "*Communication From The Commission Of the European Parliament And the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*" published 24 June 2020 (available at: https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf)

THE BROKEN SHIELD:
TOP EU COURT RESTRICTS EU-US DATA TRANSFERS

JULY 2020

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
George Mole	View Bio	george.mole@weil.com	+44 20 7903 1367