Client Alert - Data transfer: ECJ declares Standard Contractual Clauses Valid in Facebook case but strikes down Privacy Shield

Date : July 24, 2020

We first published this alert on 16 July and we've updated it with some new developments.

https://youtu.be/tePTMfNjj_4

Introduction

On 16 July the European Court of Justice ('the European Court') gave its long-awaited judgment in the latest instalment of the battle between privacy activist Max Schrems, Facebook and Ireland's Data Protection Commission.

The European Court decided that Standard Contractual which Facebook had been using to transfer data to the US were valid but that the EU-US Privacy Shield, the scheme which the European Commission put in place to replace Safe Harbor was invalid.

This ruling does not just affect the 5,378 business registered in the Privacy Shield scheme. Given the additional focus on due diligence in any data transfer every organisation will have work to do to make sure it complies.

Legal background

Transferring personal data from the EEA can only be done to countries that ensure an adequate level of data protection. Either the EU formally recognises that a country provides this protection (granting a so-called 'Adequacy Decision') or a business transferring data puts in place certain safeguards to ensure protection. The safeguards businesses most commonly rely on are so-called Standard Contractual/Model Clauses (SCCs). SCCs are a set of essentially unchangeable clauses that lay out certain privacy commitments which organisations must abide by in order to be able to transfer data, which the European Commission has pre-approved.

An alternative option for transferring data to the US has also been in place known as the EU-US Privacy Shield. The Privacy Shield scheme was introduced in July 2016 to replace a similar scheme know as Safe Harbor which the European Court had annulled in 2015 in a previous case concerning Facebook and Mr. Schrems. This case is often referred to as Schrems I. Mr. Schrems subsequently brought a second case to the ECJ in 2018 over the right to sue for damages which did not go in his favour.

What is the (third) Schrems case all about?

Mr. Schrems asked Facebook Ireland to identify the legal bases for the transfer of personal data of Facebook users from the EU to the US. Facebook Ireland referred to a data transfer processing agreement between it and Facebook Inc. (its US parent) relying on SCCs.

Mr. Schrems then brought a complaint before the Irish Data Protection Authority (the DPC) claiming that the clauses in the agreement in question were not consistent with the SCCs, and that the SCCs couldn't in any event justify the transfer of the personal data relating to him to the US.

The DPC brought proceedings before the Irish High Court which referred a number of questions to the European Court for a so-called preliminary ruling about SCCs. Some questions about the EU-US Privacy Shield were also included. There's some background on that referral here https://www.corderycompliance.com/ireland-to-refer-schrems-matter-to-european-court-for-legal-clarity-about-model-clauses/.

What did the European Court say about SCCs?

The ECJ in effect followed the preliminary advice of the Court's Advocate General Henrik Saugmandsgaard Øe (see here http://bit.ly/schremsag) in saying that nothing had been done to affect the validity of SCCs. In effect then SCCs live on but they are impacted (see below).

A key point that should also be taken on board is that is that the European Court says (in paragraphs 134 and 135) that:

"[…] as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."

The upshot of this is that it is not enough to simply have SCCs in place but that due diligence also has to be undertaken, and possibly additional protections added. That due diligence will need to be done not only on the other party to the agreement but also on the legal regime in the country where it is based.

Data protection authorities across the EU will also be expected to step up their enforcement of the data transfer requirements of GDPR including looking at how organisations are using SCCs. This comes at a time when investigations in most EU countries are on the rise.

What did the European Court say about Privacy Shield?

The European Court decided that Privacy Shield, like Safe Harbor, was invalid. Essentially, there are not enough checks and balances in US domestic law concerning the access and use by US public authorities of data transferred from the EU in a way that gives EU data subjects equivalent protection to EU law. The Court decided that the US system did not have a proportionality test for access and use of the data transferred by "US public authorities" and that surveillance in the US was not subject to a strict necessity test. The Court also said that the US Ombudsperson mechanism does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law.

In some respects this mirrors the prediction Mr. Schrems gave when we discussed the case with him in Paris in 2016 (see https://bit.ly/schremsparis). Mr. Schrems said then that "Privacy Shield is Safe Harbor with flowers on it – it will probably be killed by the European Court". The European Court clearly decided that the efforts the European Commission had made post-Safe Harbor to improve the scheme and turn it into Privacy Shield were not sufficient.

As regards the effect of the European Court's annulment of the EU Decision setting up Privacy Shield, the European Court states that:

"*As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum […], the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article*

details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR."

So are Standard Contractual Clauses safe?

No. There is no blanket protection for SCCs. As we've said organisations will have to do their own due diligence when putting SCCs in place. They will have to look both at the organisation they are transferring data too and the countries involved. This double due diligence is likely to mean that some transfers – particularly to the US given the ECJ's comments on the US legal regime – should be stopped.

Anyone using SCCs will also need to monitor developments in the countries where they have operations or interests. The case reminds DPAs of their obligations in policing SCCs and we can expect them to be more active.

What happens next?

Negotiations have already started with the US, presumably for 'Safe Harbor 3/Privacy Shield 2' or whatever it may end up being called. V?ra Jourová, who led the European Commission's negotiations with the US on Privacy Shield and who is now the Commission's Vice-President for Values and Transparency, met with Wilbur Ross the US Secretary of Commerce on Tuesday presumably to start developing a plan. Like in the film world however the sequel is rarely as good as the original and it seems that Safe Harbor 3/Privacy Shield 2 is unlikely to last as long as its predecessors given the changed data protection climate in Europe and the fact that many more organisations now exist who are prepared to challenge arrangements like this. Some of those pressure groups including La Quadrature du Net in France and Digital Rights Ireland in Ireland had also challenged Privacy Shield. The passing of GDPR also gives data subjects more ability to make their own requests and challenges.

Negotiations with the US for greater concessions may also be made more problematic by the Trump administration's unwillingness to make major concessions previously and by the fact that it is a US election year.

Mr. Schrems said after the judgment:

"*The Court clarified for a second time now that there is a clash between EU privacy law and US surveillance law. As the EU will not change its fundamental rights to please the NSA, the only way to overcome this clash is for the US to introduce solid privacy rights for all people – including foreigners. Surveillance reform thereby becomes crucial for the business interests of Silicon Valley*."

The European Data Protection Board met on 17 July 2020 to consider its initial response. Its statement said:

"The EDPS notes that the Court, while in principle confirming the validity of Standard Contractual Clauses (SCC), provided welcomed clarifications regarding the responsibilities of controllers and European DPAs to take into account the risks linked to the access to personal data by the public authorities of third countries. European supervisory authorities have the duty to diligently enforce the applicable data protection legislation and, where appropriate, to suspend or prohibit transfers of data to a third country."

It must be remembered that whilst the EDPB has a role in promoting consistency across the EU in enforcement it is up to each individual DPA to investigate and enforce. Some DPAs may start their own investigations – for example the Hamburg DPA, Johannes Caspar, suggested on 16 July 2020 that he also believed SCCs should have been struck down by the Court and we can expect him to start investigations into those organisations who still use them. The Bavarian DPA had previously conducted a survey on data transfer which could be used to start enforcement activity. The Berlin DPA has suggested that companies should look at storing data in the EEA given the concerns expressed about the US regime.

The DPC has also said that SCCs will also be under scrutiny saying:

"[The Court} has also ruled that the SCCs transfer mechanism used to transfer data to countries worldwide is, in principle, valid, although it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of

personal data to the United States is now questionable. This is an issue that will require further and careful examination, not least because assessments will need to be made on a case by case basis."

We have been monitoring statements from DPAs across the EU which do differ. Any organisation will need to factor in the views of the DPAs where they do business into their response.

Wilbur Ross has said that the US will continue to maintain Privacy Shield pending further developments and it will expect those in the scheme to do their renewals and maintain their Privacy Shield commitments.

One off-the-wall possibility might be to look at individual US States – for example will the EU try and negotiate now with California? That will be far from easy since the acts complained of are Federal and not confined to a particular State but it might not stop people trying for a deal.

Takeaways

In our view every business should work on a data transfer response plan. Even if this is a work in progress it might be something that they can show a DPA if they come knocking. It's a strategy which we used after the fall of Safe Harbor and it worked well for many then. The plan might also be something that will reassure customers, employees and other stakeholders. That plan might include:

1. Thinking about how you transfer data. If you rely on Privacy Shield you will need to look at another way – that might be a beefed-up SCC process or so-called Binding Corporate Rules (BCRs) – or in some cases both;
2. It is also important to look at how those you do business with those who have used Privacy Shield to legitimise data transfers too – for example if you have a global HR platform, a global payroll provider, a travel management company or a whistleblowing helpline they may rely on Privacy Shield. You can check to see if they are on the list here - https://www.privacyshield.gov/list If they are you'll need a new plan and it is important to contact those you do business with now – we saw after Safe Harbor was struck down that queues for assistance developed very quickly. In some sensitive areas you might want to look at securing service providers in the EEA instead;
3. In a post-GDPR world employees and customers are likely to ask questions about the way in which you make data transfers lawful. Be ready for their questions. Some prepared FAQs may help HR team and contact centres respond to these questions. Works councils are also likely to ask questions too;
4. Look at your transparency obligations. Many organisations specifically refer to Privacy Shield in their privacy policies for example – these will therefore need updating. You might need to alter other documents too including internal notices to employees and GDPR Article 30 records;
5. It is tempting to think that since the European Court has ruled that SCCs are valid, it's business as usual concerning SCCs. However, as the European Court has indicated, even where a business relies on SCCs, data protection due diligence may still be required in addition. Additionally, it is expected that under GDPR the European Commission will be revising SCCs – so businesses may at some point in the future need to adapt/update their existing SCCs; and,
6. This year, under Brexit, the UK and the EU are trying to hammer out a new relationship for the future. This should include data protection arrangements with a possible adequacy decision for the UK. The UK itself is also expected to introduce new UK data protection legislation – this can be expected to also deal with data transfers, for example we may see UK-specific SCCs and even a UK-US Privacy Shield. So businesses also need to follow these developments. Today's ruling is also likely to make the post-Brexit data protection regime significantly more challenging.

For other articles that we have written about data protection issues please see here: https://www.corderycompliance.com/news/

For details about Cordery's GDPR Navigator subscription service, which includes short films, straightforward guidance, checklists and regular conference calls to help you comply, please see here: www.bit.ly/gdprnav.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in

London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com