The Schrems II Judgement and SCCs

By Tom Hayes, BEERG Executive Director

The decision by the Court of Justice of the European Union (CJEU) to strike down the EU-US Privacy Shield **is more far-reaching** than may, at first sight, appear.

The legal transfer of personal data from the EU to the US by businesses may be coming perilously close to legally impossible. And that can only be bad for business and ordinary Europeans. There is a price to be paid for absolutist concepts of data privacy.

BusinessEurope Director General Markus J. Beyrer said:

> *"This is a blow for the whole trans-Atlantic trade. It could hurt many European companies as they continue to struggle with the COVID crisis. We cannot push a big part of transatlantic trade in limbo from one day to the other, mostly all trade is bound to the transfer of data."*

Because, not only did the court invalidate the Privacy Shield which facilitates the movement of data between the EU and the US and is used by around 5,000 companies, the Court also instructed Data Protection Authorities (DPAs) to ensure that data transferred through Standard Contractual Clauses (SCCs) is also properly protected when it arrives in the destination country.

While no figures are available, there could be many hundreds of thousands, if not millions, of data transfers out of the EU every year to non-EU countries using SCCs. Whether or not DPAs have the resources to properly monitor so many transfers is open to doubt.

As HR Policy Privacy Counsel Harriet Pearson of Hogan Lovells commented:

> *"Twenty years of streamlined data transfer compliance is now effectively over since Europe's highest court has invalidated the EU-US Privacy Shield. And with another key GDPR compliance mechanism—standard contractual clauses—under scrutiny, companies in the U.S. and globally will want to monitor the situation and to plan to confirm the legal sufficiency of the contractual arrangements they use to access European personal data."*

In summary:

- *With effect from the time of the Judgement on July 16, it is no longer legal to transfer personal data from the EU to the US relying on Privacy Shield*
- *There are also question marks over the use of SCCs, despite immediate and wide-spread comments that "SCCS are safe". They are not. They are now in a "high risk" category*
- *The ruling creates an acute "Brexit Dilemma", with the UK potentially caught between EU and US.*

In view of the legal uncertainty created by the ruling and the risk that businesses in breach of the GDPR could be fined up to 4% of their global turnover or €20m, whichever is the greater, it is vital that the European Commission and the data protection authorities provide a "breathing space" of three to six months to provide time for political and legal solutions to be found.

A fundamental clash

The striking down of Privacy Shield follows the earlier invalidation of its predecessor, Safe Harbour. The reason for both decisions is the belief on the part of the judges of the CJEU that the right to data privacy enshrined in the EU Treaties and laws is fundamentally incompatible with US national security laws, which give US intelligence agencies the right to access the data of non-US citizens, with no real right of redress on the part of an aggrieved non-US person.

The question for European policymakers must now be if there is any replacement mechanism for Privacy Shield that will withstand CJEU scrutiny? Could there be a change in US laws to accommodate European privacy concerns? The answers to both questions seem to be "no".

But if the unfettered right of US intelligence agencies to access EU citizens' data transferred under Privacy Shield, surely they have the same right to access data transferred under SCCS?

As the advocacy group, noyb, set up to support Max Schrems, the Austrian who lodged the complaint that resulted in the CJEU decision, was quick to point out:

> *IMPORTANT CORRECTION: ECJ found SCCs valid only because they cannot be used under US surveillance. SCCs are thus de facto dead for outsourcing to US companies.*
>
> *Unfortunately, many reports claim that data flows continue to be legal after SCCs and that Facebook could continue to use them. This is unfortunately incorrect.*
>
> *The CJEU has made it clear in its ruling that even within the SCCs a data flow must be stopped if a US company falls under this surveillance law. This applies to practically all IT companies (such as Microsoft, Apple, Google or Facebook) that all fall under FISA 702. Just because there is this "stop" within the SCCs that makes it impossible to use them in such cases, the SCCs were not declared invalid.*
>
> *The statement that a data flow to the USA under the SCCs remains legal is therefore wrong. This would only be possible if a US company is not subject to any monitoring laws (e.g. an airline, a bank or a retail business). Consequently this is also not a "half win", as 100% of the outsourcing that may be subject to US surveillance is not allowed - no matter if under Privacy Shield or SCCs.*

Schrems himself said:

> *"We need US surveillance reform. The Court has clarified that there cannot be any transfer of data in violation of EU law."*

Herwig Hofmann, law professor at the University of Luxembourg and one of the lawyers arguing the Schrems cases before the CJEU, said:

> "*The CJEU has invalidated the second Commission decision violating EU fundamental data protection rights. There can be no transfer of data to a country with forms of mass surveillance. As long as US law gives its government the powers to vacuum-up EU data transiting to the US, such instruments will be invalidated again and again. The Commission's acceptance of US surveillance laws in the Privacy Shield decision left them without defence*."

After ruling, the Berlin privacy regulator says companies should move personal data stored in the US to Europe. Especially companies using US cloud services should immediately switch to EU providers (or providers with EU-level privacy law) see here

EU complacent?

Responding to the Court's decision, the EU Commission **Vice-President Jourová** said:

> *In its judgment today, the Court of Justice of the European Union once again underlined that the right of European citizens to data protection is absolutely fundamental. It confirms also what the Commission has said many times and what we have been working on:* ***When personal data travels abroad from Europe, it must remain safe.***
>
> *I know citizens and businesses are seeking reassurance today on both sides of the Atlantic. So let me be clear: we will continue our work to ensure the continuity of safe data flows. We will do this:*
>
> - *in line with today's judgment*
> - *in full respect of EU law*
> - *and in line with the fundamental rights of citizens.*
>
> *We strongly believe that in the globalised world of today, it is essential to have a broad toolbox for international transfers while ensuring a high level of protection for personal data.*

Commissioner Reynders added:

> *First, I welcome the fact that the Court confirmed the validity of our Decision on* ***Standard Contractual Clauses.*** *We have been working already for some time on modernising these clauses and ensuring that our toolbox for international data transfers is fit for purpose.*
>
> *Standard Contractual Clauses are in fact the most used tool for international transfers of personal data and we wanted to ensure they can be used by businesses and fully in line with EU law. We are now advanced with this work and we will of course take into account the requirements of judgement.*

What is interesting about these remarks is that there is little in them about looking for a replacement for Privacy Shield. The emphasis is on making SCCs fit-for-purpose.

Unfortunately, irrespective of how extensively SCCs are updated they run into the problem highlighted by the Schrems group: the right of US security agencies to access data, no matter how it arrives in the US. No private US company, big and all as they may be, can give an assurance that it will safeguard the personal data of EU citizens in the face of legal demands from US agencies.

Ultimately, the problem is a political problem and not a legal one. Following the CJEU ruling the law is now clear.

Privacy Shield is dead, and any possible replacement will also likely be struck down. SCCs are now also wide-open to legal challenge and expect data privacy hawks to begin attacking them soon.

Businesses need to be aware that not only do they run the risks of fines if they are found to be in breach of the GDPR, but that data protection authorities also have the power to award compensation to aggrieved individuals who believe that their personal data has been compromised.

But as BusinessEurope Director General Markus J. Beyrer, quoted above, pointed out:

> *"mostly all trade is bound to the transfer of data".*

Modern economies run on the transfer of data and this will be even more so in the future as 5G is rolled out and the "internet of things" is built. How far does the EU want to isolate itself from the wider world behind a wall of privacy?

The law is clear. But the law results from political and social choices. To date, privacy advocates and data hawks have been in charge of the debate. But expect a backlash as and when millions of ordinary European

citizens begin to find that they cannot do things because of EU/US data blockages. When Nathalie in Dijon find problems with her Facebook page, or Manfred in Hamburg cannot participate in a Zoom call because these things run through US-based "clouds" will they say "Oh, that's OK, a price well worth paying to protect our privacy". We somehow doubt it.

The problem will be further compounded, and greatly compounded, by Brexit. Because once the UK becomes a "third country" then exactly the same problems as regards data flows between the EU and the UK will arise, as this piece from Oliver Patel makes clear.

But it could be even more complicated. Thousands of truck drivers cross between the UK and mainland Europe every day. When the Brexit border drops into place their personal details will have to be included in customs and immigrations systems for every trip they make. That is personal data.

What happens if the UK fails to get an adequacy decision because of concerns that data transferred to the UK could then be transferred onwards to the US, for example? (*We will write separately about the implications of the Schrems II judgement for Brexit).*

You cannot have it all. You cannot have unfettered data privacy and unfettered data flows between the EU and the US. Choices and trade-offs must be made. To date, to coin a phrase, politicians have been "shielded" from having to make those decisions by Privacy Shield. That shield has now been shattered by the broadsword of the CJEU.

To demand, as Schrems has done, that the US change its security laws so that a data privacy activist in Austria can continue to use Facebook is to demand the impossible.

In any case, does anyone really believe that the US intelligence agencies, and all the others, cannot access EU citizens' data when it is stored in the EU? Personally, I have always thought that the clue was in the word "spy" and James Bond never seems to be overly concerned about the legality of his activities in other countries. I suspect that the US agencies, and the British, French, German, Russian and Chinese, all take the "Bondian" approach to their work, especially when it comes to scooping up data.

And if they have the data anyway why make the access of the US intelligence community to EU data in the US a block to trade? Because demanding that governments rein in their intelligence agencies is a demand that is never going to go anywhere. Personally, I would be more concerned about that economic uses to which my data is being put by economic operators. Now, that is something governments could do something about.

One final thought. I am reminded in all of this by Prohibition in the US in the 1920s, the banning of alcohol for the most virtuous of reasons. It didn't work because people were going to drink alcohol, not matter what the law said. Drinking alcohol is just too enjoyable, and people were going to find ways of doing it. "Data Prohibition" is not going to work either because as Oliver Patel says, you can't unplug Europe from the internet.

So, the choice is clear. Unfettered EU data privacy laws will shackle EU businesses in an increasingly data driven age. Time for the EU to at least recognise the challenge.

July 2020