Articles + Publications | July 29, 2020

Locke Lord QuickStudy: Privacy Shield Struck Down: *Schrems II* – Just When You Thought it Was Safe to Go Back in the Harbor

Locke Lord LLP

WRITTEN BY

Theodore P. Augustinos | Andrew Shindler | Thomas J. Smedinghoff

RELATED OFFICES

London

16 July 2020 will go down in data protection history. On that day, the EU Court's decision in *Schrems II* dealt international data transfer a mighty blow.

The EU-US **Privacy Shield** has fallen with immediate effect.

The EU's adopted **standard contract clauses** survive, but can only be used where the destination country's laws contain safeguards of a GDPR standard.

If supervisory bodies and businesses follow this decision strictly, every day activities will require burdensome due diligence and may have to be suspended.

This has the potential to disrupt business in many sectors.

Legal Background

As everyone now knows, the EU's GDPR sets a gold standard for protecting personal data that applies in all EEA[1] countries and to many organisations in other parts of the world.

The GDPR prevents an organization transferring personal data outside the EEA unless the destination country is on an adequacy *white list* or the organization adopts an ***adequate safeguard***, except in very limited circumstances. Given the powers of EU supervisory authorities to ban unlawful data transfer and to levy large fines, up to 4% of global group turnover or €20 million, it is important to respect these rules.

Only seven major countries[2] – with due respect to Andorra and various small islands – are on the white list. However, that list is not limited to entire countries. The EU can also white list specified sectors within countries. Using this power, in July 2016 it made the important decision that U.S. organisations certified under the ***EU-US Privacy Shield*** were also white-listed[3]. This replaced its 2000 ***Safe Harbor*** decision to similar effect, which the EU Court had struck down as invalid in 2015, in *Schrems I.*

As mentioned above, organisations transferring personal data to a non-EEA destination which is not white-listed generally have to establish an ***adequate safeguard***. By far the most common of these safeguards, the easiest to establish and often the only one available, is the EU adopted ***standard contract clauses (SCC)***. The SCC are probably used by thousands of organisations around the world.

Schrems II challenged both the Privacy Shield and the SCC, striking at the heart of cross-border data transfer.

Background Facts

In 2013 Austrian law student, Max Schrems, asked the Irish Data Commissioner to prevent Facebook Ireland transferring his data to Facebook USA. He argued U.S. law didn't adequately protect his personal data, given the FBI and NSA's surveillance powers and activities.

Although this ultimately resulted in the 2015 *Schrems I* ruling that U.S. *Safe Harbor* was invalid, it did not end the argument because Facebook said most of its data transfer to the U.S. was under the SCC, not Safe Harbor. Accepting the Commissioner's invitation to reformulate his complaint, Schrems argued that once in the U.S. his data was available to the FBI and NSA under laws incompatible with the EU Charter and was not adequately protected despite the SCC.

The Commissioner agreed and brought court action in Ireland, questioning the validity of the 2010 EU decision which adopted the SCC.

The Irish Court heard evidence on the effect of U.S. national security laws. Finding these of concern, it referred the SCC question to the EU Court of Justice. For the same reasons, it also asked the EU Court to scrutinize the validity of the EU-U.S. Privacy Shield, which had been adopted in the intervening period.

EU Court's Decision on the Privacy Shield

The Court observed that the Privacy Shield was expressly stated to be subject to U.S. national security requirements, which enabled interference with the fundamental rights of data subjects. The Court went on to examine the EU Commission's justification for nevertheless approving the Shield. These are set out in a recital declaring:

"on the basis of available information about the U.S. legal order … any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred … under the Privacy Shield … for national security [or] law enforcement purposes, … will be limited to what is strictly necessary to achieve the legitimate objective in question, and there exists effective legal protection against such interference"

The Court examined FISA, the U.S. Foreign Intelligence Surveillance Act, and Executive Order 12333 on Intelligence Activities and fundamentally disagreed with the Commission's justification. The Court found U.S. surveillance programs under these laws enabled agencies such as the FBI and NSA to access personal data transferred from the EU to the U.S. without limitation and without guarantees for non-U.S. individuals. Ultimately, it concluded that U.S. laws:

- limit the protection of personal data in ways which are not restricted in a manner equivalent to EU law requirements,

and

- do not grant data subjects actionable legal rights against U.S. authorities.

Consequently, it had no hesitation in finding the Privacy Shield invalid, with immediate effect.

EU Court's Decision on the SCC

The Court's decision on the SCC was more nuanced. Its key finding, which will be a relief to business, is that the EU Commission decision approving the SCC was valid. However, the Court applied a significant qualification, ruling that the SCC can only be used where data subjects are given a level of protection equivalent to GDPR in the destination country.

Applying this qualification, the judgment directs EU data protection authorities to suspend or prohibit data transfer using the SCC where the law of the destination country does not provide appropriate safeguards, rights and remedies against access by national authorities.

Organizations concluding from this that they can carry on using the SCC until an authority stops them will be disappointed. The judgment goes on to declare every entity transferring personal data out of the EEA under the SCC responsible for assessing whether the destination country's law ensures adequate protection. They must do so on a case by case basis, before they make any further transfer.

The burden does not stop at the data exporter: the Court also pointed out that the SCC themselves require the data importer to notify the exporter if it cannot comply, including where public authorities in its country can access the data disproportionately or without redress. The Court ruled that transfer must stop if the exporter receives such notification.

Finally, the Court suggested a data exporter could take "*adequate additional measures to guarantee protection*" if the destination country's laws did not pass the assessment. However, short of persuading that country to change its laws it is difficult to see what such measures could be: while the exporter could insist on additional contractual safeguards with the importer, these will have no effect on public authorities in the destination country, which are not party to the SCC.

Effects of the Decision

Data Transfer to the U.S.

Data transfers under the Privacy Shield are now unlawful. Although authorities are unlikely to take immediate enforcement action, such as banning transfers and levying fines, businesses should find an alternative basis for transferring personal data to the U.S. as soon as possible, since any informal "*grace period*" will not last long.

Ideally, the alternative basis for transfer will involve using an *adequate safeguard*. The obvious solution would have been to use the SCC – commonly used to transfer data to U.S. organisations not certified under the Privacy Shield. But given the EU Court's combined findings on the use of the SCC and on U.S. laws, it seems inevitable that this will not withstand further scrutiny.

Apart from the SCC, the only other *adequate safeguard* readily available to private organisations is to use *binding corporate rules*, but these apply only within a corporate group and so are of no use for transfers between independent entities. They also require bespoke drafting and regulatory approval.

In the absence of the Privacy Shield and without an adequate safeguard, organisations can generally only transfer personal data to the U.S. on a repeated basis with the explicit consent of the data subject or where necessary for a contract[4]. Even one-off transfers will require justification and regulatory notification.

The use of consent is therefore likely to increase. This will often be onerous and will need careful management, since the GDPR also has strict rules on consent. If data subjects refuse consent, and every data subject is entitled to refuse, one can foresee major problems.

Data Transfer to other Non EEA Countries

Most data transfers to non-white-list countries take place under the SCC. Applying *Schrems II* strictly, every EU data exporter using the SCC must now assess the laws of the destination country, if necessary with the help of the importer, before carrying out further transfer.

This assessment should include a focus on law regarding access by public authorities in the destination country, in particular whether their access is proportionate and whether data subjects have actionable legal rights against them.

Having assessed the relevant foreign law, unless the exporter finds it as protective as GDPR and consistent with the EU Charter, it must end the transfer. There must be a significant concern that many, if not most, countries will fail this assessment. Where that is so, the position will be the same as for the U.S.

EU data protection authorities are required to enforce the GDPR with all due diligence. Strictly applying *Schrems II*, they must suspend or ban personal data transfer to third countries under the SCC where it cannot be protected to EU standards, unless the data controller has already put an end to the transfer. In the coming months, we may see decisions from the authorities that the SCC cannot be used for certain named countries.

Conclusions

Strict observance of the EU Court's decision in *Schrems II* will disrupt current practice in international data transfer from the EU.

How many nations, other than the handful currently on the white list, have data protection laws equivalent to GDPR? How many nations circumscribe the activities of their intelligence and national security authorities and give foreign nationals individual legal rights against them? Indeed, there are doubts about the UK receiving a white listing following Brexit for that very reason. Even existing white list decisions are subject to periodic review and could be challenged at any time.

Until now, use of the SCC was the oil on the wheels of the EU data export system. If *Schrems II* is rigorously applied this will no longer be the case. This is problematic since swathes of businesses rely on transferring personal data from the EU to the U.S. and other major trading nations without specific authorization or individual consents. If *Schrems II* effectively prohibits this, then other countries may take a *tit for tat* approach, particularly

since national security laws in EU Member States may not meet the standard the EU court is expecting of other countries.

The solution may have to be political, but as both Schrems cases show, political solutions may not withstand the scrutiny of a court. Ideally, *Schrems II* will lead to a world-wide standard of data protection equivalent to GDPR, but that seems a long way off and is probably unachievable given the primacy countries give their national security.

Until a solution is found, businesses that export or import data are likely to have to make changes to their practices and legal arrangements. The only consolation, although a poor one, is that everyone is swimming in the same choppy waters.

Recommendation
We recommend that organisations which export or import EU personal data take urgent legal advice on the best way forward.

For more information, please contact the author.

---

1 The EU countries plus Norway, Iceland and Lichtenstein. ?

2 Argentina, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay.

3 ?A similar decision has been made for in Canada for commercial private-sector organizations. ?

4 The other exceptions are extremely narrow, e.g. for legal claims or matters of life or death. ?

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Privacy + Cyber