CJEU judgment in Schrems II: International Transfers Under Threat: Privacy Shield invalidated; Model Clauses survive but need review

July 16, 2020

Introduction

Earlier today, the Court of Justice of the European Union (CJEU) handed down its long-awaited judgment in the *Schrems II* case (Case C 311/18). See also the CJEU press release here. The landmark case was triggered by a request for a preliminary ruling submitted by the Irish High Court, in the context of a case brought by the Irish privacy regulator (the DPC).

At the heart of the case before the CJEU was the question of whether the EU standard contractual clauses for transfers of personal data from controllers based in the EU to processors based outside the EU (Commission Decision 2010/87/EU) (the SCCs or Model Clauses) are a valid mechanism for lawfully exporting personal data from the EU, given the possibility that the national security and law enforcement authorities at the destination country may oblige the data importer to disclose the EU personal data to them. Furthermore, the case also extended to the question of the validity of another key EU data exports mechanism – the EU-US Privacy Shield (Decision 2016/1250).

The Model Clauses are the most widely used mechanism for exporting personal data from the EU. The EU-US Privacy Shield is relied on by thousands of companies on both sides of the Atlantic to legitimise EU-US data exports. More than 5,000 US companies are registered under the scheme. It is also worth noting that, since 2015, many organisations have had to update their EU data exports arrangements twice to respond to changes in EU legal requirements: first, in 2015, following the invalidation of the EU-US Safe Harbour (the predecessor of the Privacy Shield) and then again, in 2018, as a result of the GDPR (which requires specific language in contractual arrangements between controllers and processors). The prospect of a CJEU judgment that potentially invalidates up to two of the main EU data exports solutions and, therefore, requires a similar exercise for the third time in six years caused concern for many organisations, especially at a time of major economic uncertainty.

Perhaps unsurprisingly, the final outcome is a mixed picture, but these concerns have partly materialised. In short, the CJEU held that:

- the **SCCs remain valid** but the CJEU emphasised the requirements that organisations will need to satisfy in order to be able to rely on the SCCs moving forward, namely carrying out an assessment of the level of protection in the destination country, taking into consideration both the contractual clauses agreed between the EU data exporter and the non-EU data importer and, with regards to any access by the public authorities of the destination country to the data transferred, the relevant aspects of the legal system of that third country. This will not be a straightforward assessment for many organisations, and the result may be that organisations may be able to rely on SCCs for some third countries but not others;
- unless there is an adequacy decision for the destination country, EU privacy regulators are required to suspend or prohibit a transfer of personal data to a third country where they take the view that the SCCs are not or cannot be

complied with in that country and that the protection of the data required by EU law cannot be ensured by other means, where the EU data exporter established in the EU has not itself suspended or put an end to such a transfer; and

- **the EU-US Privacy Shield is invalid** because the requirements of US national security, public interest and law enforcement have primacy and, therefore, condone interference with the fundamental rights of persons whose data are transferred to the US. Furthermore, US domestic law does not provide protections that are essentially equivalent to those under EU law.

Below we provide a summary of the key points of the judgment and our immediate assessment of what it means in practice.

The CJEU judgment

As far as the SCCs are concerned, the CJEU, in essence, agrees with the AG and confirms the validity of the SCCs as a lawful basis for exporting EU personal data, but with certain caveats and conditions, the most important of which are:

- the existence of signed SCCs does not prevent national Supervisory Authorities from investigating claims in connection with the SCCs and they have the power to prohibit or suspend a data transfer or a set of transfers where they find that EU data is not adequately protected. The CJEU appreciates that this may result in the Supervisory Authorities in the various member states adopting divergent decisions. In order to manage this, the CJEU points to the consistency mechanism under the GDPR on the basis of which the Supervisory Authority considering the prohibition of transfer to a particular third country can refer the matter to the EDPB for an opinion which will, in turn, be able to adopt a binding decision for all supervisory authorities;
- controllers seeking to rely on the SCCs should, prior to any transfer of personal data, carry out due diligence to assess whether the local law of the destination country provides a level of protection that is essentially equivalent to that provided under the EU data protection regime. This also involves carrying out an assessment to confirm that the law of the destination country does not impose any obligations on the importer which are contrary to the importer's obligations under the SCCs (for example, they should confirm that the importer, under its local law, will be able to ensure adequate level of protection against access by the public authorities to that data). It is too soon to tell whether SCCs will be unavailable for use with respect to some countries due to an inadequate level of protection against access by the public authorities to data.
- Following the transfer of data:
- both the exporter and the importer should ensure that the processing of that data has been and will continue to be carried out in accordance with EU data protection law; and
- in particular, the data importer should inform the exporter of any inability to comply with the SCCs, and the exporter is, in turn, obliged to suspend the transfer of data and/or to terminate the contract.
- Where special categories of data could be transferred, the exporter (as it is already required under the SCCs) should inform the data subject before, or as soon as possible after, the transfer to enable the data subject to be in a position to bring legal action against the exporter so that the exporter suspends the proposed transfer, terminates the contract concluded with the recipient of the personal data or, where appropriate, requires the recipient to return or destroy the data transferred.

In other words, the CJEU re-emphasised existing requirements of pre-contractual due diligence and ongoing monitoring of the importers' compliance and the legal regime in the destination country. These are the mechanisms which the CJEU pointed to as being in existence that exporters must use to ensure that "appropriate safeguards" are in place to protect transferred data. However, to date, not much emphasis was paid to these requirements in practice, with many organisations treating the entering into SCCs as a "paper" exercise. This will likely change moving forward. We should anticipate that European Supervisory Authorities will have cause to focus on this more – through complaints on their own regulatory initiative.

The CJEU also held that the EU-US Privacy Shield is invalid effective immediately, because the requirements of US national security, public interest and law enforcement have primacy. This means it effectively anticipates interference with the fundamental rights of persons whose data is transferred to the US. The CJEU held that the limitations on the protection of personal data arising from US domestic law are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law. In other words, they do not give sufficient protection to EU citizens. In particular, the CJEU points to the fact that US law does not grant data subjects actionable rights before the courts against the US authorities. It also cites the fact that the Privacy Shield Ombudsperson mechanism is not sufficient – it 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 particular, it is not sufficiently independent and the Ombudsperson's lacks of power to adopt decisions that are binding on the US intelligence services. It is not clear whether further EU-US negotiations would result in sufficient changes to US national security laws to address these concerns.

What this means in practice

The CJEU invalidated the EU-US Privacy Shield and re-emphasised the requirements for lawfully relying on the SCCs by clarifying that it is not enough simply to rely on signing the SCCs to legitimise data exports.

The judgment emphasises the importance of the requirement on the data exporting controllers to satisfy themselves that they can rely on the SCCs. This has significant practical implications for organisations. A key part of attaining this level of assurance is that exporting controllers are expected to assess whether the legal regime of the destination country provides adequate protection for EU personal data. This should extend to, among other things, an assessment of the national security and surveillance laws of the destination country. This will likely be a complicated legal exercise even for sophisticated and well-resourced organisations, given the complexity, divergence from country to country and the relative secrecy surrounding aspects of law and practice in these areas. For companies relying on SCCs to transfer personal data to the US such an assessment may have become problematic. The EU-US Privacy Shield was invalidated on the grounds that US law is incompatible with EU fundamental rights. This suggests that a data importer in the US may not be able to protect personal data in accordance with its obligations under the SCCs.

Given the judgment's emphasis on the consistency mechanism, it remains to be seen whether the European Data Protection Board will offer leadership here in providing practical guidance for organisations undertaking these assessments or give its own assessment of "high-risk" destinations.

The judgment will have immediate effect on any existing or new cross-border data flows originating in the EU (including from the UK). In short, organisations (including exporters and importers) will need to revisit existing data export activities under the SCCs and consider whether further assurance should be sought to assess whether those transfers continue to provide appropriate safeguards. The same holds true for the new data processing activities. If the organisation has a written policy and/or process for exporting EU personal data, these will need to be updated. Such a policy would be sensible to develop now, if not already in place. In addition, organisations should revisit the data export activities currently performed under the Privacy Shield to identify and implement alternative data export

solutions (which, in most cases, will be the SCCs).

In short, the key steps that organisations need to take now include:

- socialising the issue with key business stakeholders and keeping it on the agenda;
- monitoring developing regulatory guidance;
- analysing the in-scope data export operations and:
- identifying which of them are currently performed under the EU-US Privacy Shield and plan for transition to an alternative solution – most likely SCCs;
- identifying which of them are performed under the SCCs and of those which require additional due diligence on the data importer and local law of the destination country in order to be able to rely on the SCCs in principle; and/or
- identifying suitable alternatives to the SCCs (such as an EU adequacy decision, a derogation under the GDPR for non-systematic/one-off data transfers or Binding Corporate Rules, when available) and what steps should be taken in order to be able to rely on them; or
- exploring whether changes in the technological set-up might ensure that there are no data transfers (including remote access of EU personal data from) outside the EU. However, this may not be practicable (e.g. for cloud or AI solutions).
- If it is decided to continue relying on the SCCs, the following key steps should be taken:
- designing the due diligence process to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned (who will carry it out, how, what tools (questionnaires, technology, etc.) will be used, how will it be documented and kept on file). It is likely that at least some service providers/data processors outside the EU, such as the major outsourcers and cloud service providers, will take steps to help their customers/exporting data controllers satisfy this requirement, e.g. by preparing their own assessments of the relevant local laws and/or providing "transparency" reports concerning their disclosure obligations;
- considering what additional accountability measures you should have in place to provide additional safeguards regarding "at risk" data transfers – data minimisation and pseudonymisation; DPIAs; internal international transfer policies etc.;
- preparing a remediation action plan for existing in-scope data export activities that require additional due diligence. It may also be necessary to update relevant internal policy and guidance concerning pre-contractual due diligence (e.g. in data protection policies and procurement policies) and/or privacy notices; and
- if this has not been done previously, carrying out the due diligence required for existing data exports activities. For new data export activities, carrying out and documenting the pre-contractual due diligence on the data importer and local law of the destination country.
- If it is decided not to continue relying on the SCCs, the following key steps should be taken:

- analysing the in-scope data export operations and identifying suitable solutions (such as an EU adequacy decision, a derogation under the GDPR for non-systematic/one-off data transfers or Binding Corporate Rules, when available) and what steps should be taken in order to be able to rely on them;

- planning how the new data exports solution(s) will be implemented – for instance, how assessments and analyses will be documented, written agreements will be revised (and potentially re-negotiated), how data protection policies, privacy notices and data processing records will be updated; and

- implementing the new data export solution for existing data processing activities. For many organisations, this could be a significant operational exercise that requires efficiency, cost effectiveness, automation and assurance.

As a side note, the United States Department of Commerce vowed to continue processing submissions for self-certification and re-certification under the Privacy Shield, and reminded participating organizations that the ruling does not relieve them of their Privacy Shield obligations.

In addition, organisations should factor in two imminent developments. The first is Brexit, in the context of which organisations that import EU data into the UK or export UK data to the EU and beyond will need to consider which data export solutions to implement. The second development is the new GDPR-ready version of the SCCs, on which the EU Commission is currently working, which will need to be incorporated into existing and future EU data export arrangements that rely on the SCCs.

Conclusion

Many EU data exporters and data importers, especially those based in the US, will be rightly thinking "here we go again". In the middle of an unprecedented economic crisis, data exporting and data importing organisations have to review their data exports and imports arrangements to identify alternative solutions for transfers based on the EU-US Privacy Shield. They also have to satisfy themselves that, when they rely on the SCCs, they comply with the re-emphasised requirements for pre-contractual due diligence and ongoing monitoring – all at a time when we expect the revised GDPR-ready SCCs, regulators and privacy activists will likely be paying closer attention to data exports.

In the following weeks and months, we will no doubt have further developments in this area, including statements and/or guidance from the EU Commission, the EDPB and national Supervisory Authorities which will provide more indications about their expectations, further guidance for businesses regarding the available data exports options and the timeframe for implementing them, and their views regarding the level of protection in certain third countries. These will undoubtedly take into account the status of the GDPR-ready version of the SCCs which, hopefully, will now be expedited. We may also see market practice developing around transfers to certain locations and we can expect that major vendors will put forward proposed solutions to their customers, largely based on SCCs or BCR.

It is too early to speculate on the potential enforcement risk with which organisations that fail to adapt their data exports arrangements are faced. It is reasonable to expect that there will be a grace period to enable organisations to transition to new arrangements. It is also questionable whether data exports will be a top enforcement priority for EU privacy regulators, whose attention is currently focused on other matters. Note, however, that it is possible that the CJEU judgment could encourage privacy activists to file complaints to Supervisory Authorities and/or lawsuits requesting the suspension of EU data transfers based on the SCCs. This is likely to mean regulators face more pressure to act here.

In the medium to longer term, we may also see the EDPB and/or national Supervisory Authorities launching country-specific investigations and issuing "local decisions" on data transfers to particular countries and/or preventing the use

of SCCs for EU data exports to certain countries. Finally, it will be interesting to see whether the approach that will be taken by the UK Supervisory Authority (the ICO) will be aligned to or will diverge from that of the EU EDPB and national Supervisory Authorities.

The Dentons team is digesting the CJEU judgment and will follow up on this client alert, including by way of a podcast which will be available in the next few days. If you wish to discuss any aspect of the CJEU judgment, what it means for your organisation and how we can help, please get in touch with any of the Dentons Privacy and Cybersecurity contacts listed or your usual contact at Dentons.

Your Key Contacts

Antonis Patrikios
Partner, London
D +44 20 7246 7798
M +44 7919 491029
antonis.patrikios@dentons.com

Chantal Bernier
Of Counsel, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Hakki Can Yildiz
Senior Associate, London
D +44 20 7246 7327
M +44 7795 618231
HakkiCan.Yildiz@dentons.com

Todd D. Daubert
Partner, Washington, DC
D +1 202 408 6458
M +1 202 436 1819
todd.daubert@dentons.com

Nick Graham
Partner, London
D +44 20 7320 6907
M +44 7795 618 315
nick.graham@dentons.com

Giangiacomo Olivi
Partner, Milan
D +39 02 726 268 00
M +39 344 27 62 550
giangiacomo.olivi@dentons.com

Monika Sobiecki
Senior Associate, London
D +44 20 7320 6342
monika.sobiecki@dentons.com