ALERT MEMORANDUM

Schrems II: The CJEU Declares EU-U.S. Privacy Shield Invalid, Upholds the SCCs And Calls On 27 Supervisory Authorities to Ensure Their Compliance

July 17, 2020

In a highly-anticipated landmark judgment handed down on July 16, 2020, the Court of Justice of the European Union (the "**CJEU**") in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("***Schrems II***", summarised in part 3. below and the full text of which can be accessed here) has:

— invalidated the European Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Data Protection Shield (the "**EU-US Privacy Shield**") for transfer of personal data from the EU to entities certified under the mechanism located in the United States;

— upheld the European Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established outside the EU (the "**SCCs**"); and

— reminded that a transfer of data based on SCCs may be challenged before the competent supervisory authority, which has to "suspend or prohibit", on a case-by-case basis, any such transfer when, in its view, the SCCs "are not or cannot be complied with."

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

PARIS

Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

BRUSSELS

Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

LONDON

Natalie Farmer
+44 20 7614 2309
nfarmer@cgsh.com

Mark Gwilt
+44 20 7614 2313
mgwilt@cgsh.com

1. Key Takeaways

The EU-U.S. Privacy Shield suffered the same fate as its predecessor, the EU-U.S. "Safe Harbor" framework. On the positive side, the CJEU has now clearly acknowledged that SCCs constitute a valid ground for transferring personal data outside the EU. However, using the SCCs comes with strings attached.

Following the opinion of Advocate General Saugmandsgaard Øe,[1] the CJEU places the onus on the parties contemplating entering into SCCs to first check that the country to which the data would be exported does not impose restrictions on the data importer that adversely affect compliance with the SCCs. This analysis is not only complex, it will also need to be regularly updated depending on legal changes in the concerned country.

In light of the CJEU's assessment of the deficiencies of the United States' personal data protection regime (including the Foreign Intelligence Surveillance Act (FISA) applicable to telecommunications companies or companies using their services such as cloud services), some are speculating that it is only a matter of time until transfers of personal data to the United States based on the SCCs will be prohibited. Without the need to anticipate such a broad and dramatic outcome at this stage (since not all US companies are subject to these rules), it seems certain that activists like Mr. Schrems will pursue further actions before supervisory authorities, in particular the Irish Data Protection Commission (the "**Irish DPC**"), to see transfers of personal data to the United States suspended or prohibited, but on a case-by-case basis this time.

The CJEU further stresses that it is incumbent upon supervisory authorities to ensure the legality of transfers made pursuant to SCCs, not only as regards the assessment of the legal regime of the country where the data will be exported, but also the actual compliance by the parties with the terms and conditions of the SCCs. While the *Schrems II* judgment will undoubtedly cause a greater degree of scrutiny on type of cross-border data transfers, it does not, in fact, seem to alter or increase the powers and responsibilities of supervisory authorities in that respect.

2. Practical Consequences

For companies that relied on the EU-U.S. Privacy Shield.

— Although each supervisory authority has some discretion on the timing of its enforcement of *Schrems II* in its jurisdiction, there is officially no grace period to cease transferring personal data to US companies certified under EU-U.S. Privacy Shield. These companies, and EU companies that send personal data to them, will need to promptly reconsider the way in which these transfers occur. The following alternatives will be available to them:

- Although challengeable, transfers pursuant to SCCs remain valid and might still be a vital alternative in certain cases.
- Derogations provided by Article 49 of the GDPR (such as transfers based on the consent of data subjects or necessary for the defence of a legal claim or a public interest) constitute alternative methods to transfer personal data but should be examined on a case-by-case basis. It would often be impractical to replace transfers based on EU-U.S. Privacy Shield with a derogation, given that the former was intended to cover regular data transfers whereas the Article 49 derogations are generally intended to cover transfers which are occasional and not repetitive (as confirmed by the European Data Protection Board (the "**EDPB**") in its guidance).
- In the longer term, when intra-group data transfers are contemplated, using binding corporate rules ("**BCRs**") should be considered, although they may take some time and a significant investment to put in place. BCRs must be pre-approved by the competent supervisory authority, therefore transfers under the BCRs can be presumed valid so long

[1] Opinion of Advocate General Saugmandsgaard Øe, http://curia.europa.eu/juris/document/document.jsf;jsessionid=4C1BF8AA9FA853F912613560F09B56A4?text=&docid=221826&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=9814941

as parties continue to comply with their requirements. Reasoning by analogy with the *Schrems II* judgment regarding the SCCs, strict compliance with the BCRs will be required to avoid any question as to the validity of the transfers they contemplate.

— It is unlikely that another such framework as the EU-U.S. Privacy Shield will be put in place in the near future until the EU and US data protection regimes are more closely aligned. Despite efforts being made in certain US states such as California, this seems a long way off at the federal level.

For companies relying on SCCs

— Where an EU company is using, or contemplates using, SCCs, it will have to carefully assess the legal system of the country to which it intends to transfer personal data. If the laws of this jurisdiction do not enable the party to which the data would be sent to comply with material terms of the SCCs, the transfer will be open to challenge. The CJEU suggests that the parties may establish additional safeguards to remedy these issues, but it is not evident what those could be and it may be risky to rely on untested additions to the SCCs. This is a complex analysis and places a great deal of responsibility on the parties to the SCCs. It is particularly onerous given then sizable fines under GDPR for non-compliance and the potential to have to compensate data subjects where they can demonstrate they have suffered damage in connection with the violation.

— It will be important to monitor the guidance and decisions of EU data protection supervisory authorities that are tasked with determining whether the SCCs provide appropriate safeguards in the context of the recipient jurisdiction. Given its current jurisdiction over several US technology giants such as Facebook, the Irish DPC will have a particular role to play in that regard. As noted by the CJEU itself, there is risk of possible discrepancies between the assessments of 27 different supervisory authorities. The EDPB, whose role is to ensure the consistent application of data protection rules throughout the EU, should therefore be called to step in to provide guidelines when assessing the transfer of personal data to third countries based on SCCs.

— In the event of transfers to organisations that may not be able to fully comply with the terms and conditions of the SCCs, Article 49 derogations for occasional and non-repetitive transfers or BCRs for intra-group transfers should be considered.

Post-Brexit transfers of personal data from the EU to the UK

— While the United States is immediately in the spotlight, we may also see supervisory authorities scrutinising the legal regimes and surveillance practices of other jurisdictions in particular where they habitually share data with the United States, including the UK after the end of the Brexit transition period, which is due to expire at the end of this year (in particular if the European Commission does not issue an adequacy decision in the UK's favour).

3. Summary of the CJEU Judgment

The CJEU held as follows:

— That the GDPR must be interpreted as applying to transfers of personal data for commercial purposes from an organisation in the EU to an organisation in a third country, irrespective of whether at the time of the transfer or thereafter, that data is liable to be processed by the authorities in that third country for purposes which are outside the scope of the GDPR (i.e., public security, defence and state security).

— The GDPR's requirements regarding "appropriate safeguards" for transfers of personal data to third countries must be interpreted as requiring that the data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the EU under the GDPR, read in the light of the Charter. Any assessment of the level of protection afforded in the context of a transfer to a

third country must, therefore, take into account (1) the contractual clauses agreed between the transferor and transferee established in the third country *and* (2) any access to the transferred personal data by the public authorities of that third country as well as the relevant aspects of the legal system of that third.

— The validity of the Commission's decision regarding the SCCs is not called into question by the mere fact that the SCCs do not bind the authorities of the third country to which data may be transferred. The validity of the SCCs depends on whether the decision includes effective mechanisms to ensure a level of protection required by EU law. The SCCs do establish such mechanisms, including that they impose obligations on data exporters and data importers to verify, prior to any transfer, whether an appropriate level of protection can be respected in the third country concerned (with the data importer being required to inform the data exporter of any inability to comply with the SCCs, with the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former). Supervisory authorities are also *required* to suspend or prohibit a transfer of data to a third country pursuant to SCCs, if it determines that the SCCs cannot be complied with in that third country and where personal data transferred cannot be protected as required by EU law, including the GDPR and the Charter.

— The European Commission decision implementing the EU-U.S. Privacy Shield is invalid on the basis of the following reasoning:

- The requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country.
- The limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the EU to that third country, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary.
- While the EU-U.S. Privacy Shield decision includes requirements with which the US authorities must comply when implementing surveillance programmes, the provisions do not grant data subjects actionable rights before the courts against the US authorities.

…

CLEARY GOTTLIEB