# EU DATA PROTECTION: STANDARD CONTRACTUAL CLAUSES MAY HAVE BEEN CONFIRMED BY THE CJEU, BUT AT WHAT PRICE?

Date: 17 July 2020

**EU Data Protection, Privacy, and Security Alert**

By: Claude-Étienne Armingaud, Laure Comparet, Violaine Selosse

The long awaited Schrems II decision[1] was published by the Court of Justice of the European Union (CJEU) on 16 July 2020, and while it has already been summarized as the death blow to the Privacy Shield framework and the confirmation of the validity of the Standard Contractual Clauses (SCCs) by many, it may only be a Pyrrhic victory for the latter, as far as transfers to the United States are concerned.

## WHAT ARE SCCS?

The SCCs are sets of model contract which needed to be executed, originally, between an EU based data exporters and a non-EU-based data importers, aiming to protect personal data sent from the European Union (EU) and European Economic Area (EEA) to recipients located in countries deemed as offering a level protection of the rights and freedoms of individuals lower than the EU/EEA .

Under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive) and as of today, the European has issued three sets of SCCs:

- Two sets of SCCs addressing data transfers from EU controllers to non-EU controllers:
  - Decision 2001/497/EC in which both parties enter into a joint and several liability for the data protection obligations; and
  - Decision 2004/915/EC, developed in cooperation with different trade associations and providing for more flexibility for onward transfers by the data importers; and
- One set addressing data transfers from EU controllers to non-EU processors (Decision 2010/87/EU).

Since their publication, SCCs have been widely favoured to govern data transfers, as they are considered to be a more flexible and cheaper alternative to other data transfer mechanisms, such as Binding Corporate Rules.

## WHY WERE THEY CONTESTED?

Notwithstanding any additional commercial terms which may be added by the parties, SCCs are supposed to be used “as is,” with no modifications by the parties other than their appendices, and any amendment to the published version would require a submission to a Supervisory Authority for prior approval.

They however predate GDPR[2] and have not been updated since GDPR came into force on 25 May 2018. In addition to the now-obsolete references to the Directive, the SCCs came from a period of time where EU data protection only applied to EU-based entities.

However, the extra-territorial scope of GDPR (see our analysis here) can now subject non-EU companies, who had to rely on ill-adapted SCCs to facilitate their data transfers even within their own jurisdictions.

In addition, the flexibility offered by the SCCs often translated into documents which were executed, sometimes by reference, without being duly completed and/or updated -- as easily signed as they were forgotten.

Max Schrems, the Austrian "datactivist" whose names is already associated to the CJEU decision (*Schrems I*) which invalidated the Safe Harbour mechanism on 06 October 2015 (see our coverage here), had filed a complaint to the Irish Data Protection Authority (Data Protection Commissioner or DPC), regarding Standard Contractual Clauses and the Privacy Shield mechanism, which alleged that:

- the United States did not offer sufficient protection for the data transferred in that country, due to legally mandated access to the data by U.S. authorities such as the national Security Agency (NSA) and the Federal Bureau of Investigation (FBI); and
- communication of EU data subject's personal data to U.S. governmental agencies in the context of various monitoring programs was incompatible, with articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union on the respect of private and family life, to protection of personal data and to the right to an effective remedy and to a fair trial. As a consequence, Schrems argued that, under those circumstances, the SCCs could not be used as a legal basis to transfer personal data to the United States. In particular, Schrems invoked the fact that SCCs are not binding on U.S. authorities.

The DPC considered that the outcome of Schrems' complaints depended, in particular, on the validity of the SCCs resulting from Decision 2010/87 and that the assessment of the validity of the Privacy Shield Mechanism (Decision 2016/1250) was to be decided at EU, rather than national level.

## THE POSITION OF THE CJEU

Today's decision contains a wealth of important information.

### The SCCs as a template to customize on the basis of the importer's location

In addition to invalidating the Privacy Shield framework (see our alert here) the CJEU elected to uphold the SCCs as a valid mechanism of general availability to entities subject to GDPR. In its decision, the Court considered that, when drafting and approving SCCs, the European Commission did not necessarily have to provide all the appropriate safeguards required by Art. 46 GDPR.[3]

Indeed, the Court recognized that "it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards."[4] This means that the onus of ensuring that the personal data transferred outside of the EU/EEA is and remains adequately protected bears onto the data exporting entity.

In addition, the CJEU added that since the SCCs themselves cannot, by nature, bind the public authorities of third countries in which the data importer is located, but only their signatories, "it may prove necessary to supplement the guarantees contained in those [SCCs]."

Both data exporters and data importers will therefore have to verify on a case-by-case basis "whether the law of the third country of destination ensures adequate protection under EU law, of personal data transferred pursuant to [SCCs], by providing, where necessary, additional safeguards to those offered by those [SCCs]."[5]

As a consequence, the SCCs should be construed as a generic baseline for transfers to any third country not offering an adequate level of data protection, but, depending on the location of the data importers, supplemental terms taking into account the data importers' legal framework may be required to warrant sufficient safeguards over the data.

## The SCCs mandates the immediate suspension of data transfers in case the parties can no longer comply with them

In the case where no additional measures would be able to guarantee such protection, the data exporter will need to suspend the transfer of data (or risk being in breach of its undertakings under GDPR). Such situation would notably arise when "the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those [SCCs] 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."[6]

When receiving such notice the controller is bound to suspend the transfer of data and/or terminate the contract with the recipient. If it decides despite such notice to continue the transfer, the controller will then have to notify the competent Supervisory Authority which has the right to conduct an audit and "to suspend or prohibit the transfer of data if the clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means."[7]

The Court notably relied on Clause 5 of the SCCs, which requires the data importer to notify the controller if it becomes unable to comply with the SCCs due to, inter alia, the legislation of the country where the importer is established (e.g. transfer of data to governmental agencies and when such transfer goes beyond what is necessary for the purposes of national security, defense and public security[8]).

## The extraterritorial effect of GDPR, again

Finally, it is worth noting that the CJEU, interpreted that Clause 5 of the SCCs as biding on the non-EU based data importer even if the law applicable in the jurisdiction in which it is established would prevent disclosure of the communication of the personal data by the importer to the law enforcement authority: "Furthermore, although Clause 5(d)(i) allows a recipient of personal data not to notify a controller established in the European Union of a legally binding request for disclosure of the personal data by a law enforcement authority, in the event of legislation prohibiting that recipient from doing so, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the recipient is nevertheless required, pursuant to Clause 5(a) in the annex to the SCC Decision, to inform the controller of his or her inability to comply with the standard data protection clauses."[9]

Consequently, while the data importer will not need to go into the specifics, it will need to refrain from further processing of the transferred data. It remains to be seen to what extent this requirement will effectively lead to non-EU data importer to spontaneously put an end of the data transfer which are often an accessory to the services they perform for their partners.

## WHAT DOES IT MEAN?

As initially highlighted by the DPC, transfers of personal data from the EU to the United States are inherently problematic, regardless of the legal mechanism by which such transfers are conducted.

Today, the CJEU has officially stated that United States were not offering adequate protection due to interference of its governmental agencies, and invalidated the existing data transfer mechanism. It is clear that SCCs, as currently available, cannot, by themselves, sufficiently safeguard any data transfers to the United States.

Indeed, the use of SCCs is now contingent on the case-by-case verification by the data controller of the adequacy of the law of the country to which the data is transferred - with already a presumption that that of the United States will require additional contractual safeguards.

There seems to be no way out of this conundrum, except if by moving away from SCCs altogether.

## WHAT HAPPENS NOW?

The full extent of the practical consequences for companies remains uncertain at this stage: in the absence of updated templates approved by the European Commission, companies may need to move toward ad hoc data transfer agreements which will need to be approved by local Supervisory Authorities. This could potentially create a fragmentation of the harmonization expected under GDPR and potential forum shopping for data transfers within the European Union.

Vera Jourova, who leads the European Commission's effort on Values and Transparency, has stated today that the Commission will now work with Member States Supervisory Authorities to update data-transfer mechanisms in the wake of the Schrems II ruling, thereby answering a call from professionals and businesses for such action since 2016.

However, now may also be the time for industry sectors to consider alternatives to data transfer mechanism, such as codes of conduct and certifications (see our alert on Codes of Conduct here).

K&L Gates global data protection team (including in each of our European offices) remains available to assist you in achieving the compliance of your data transfers at global levels.

# FOOTNOTES

[1] Court of Justice of the European Union - Grand Chamber - 16 July 2020 - C-311/18 - *Schrems II*

[2] General Data Protection Regulation 2016/79 dated 27 April 2016, which enter into force on 25 May 2018 (GDPR)

[3] Case C-311/18 Point 128

[4] Case C-311/18 Point 131

[5] Case C-311/18 Point 134

[6] Case C-311/18 Point 135

[7] Case C-311/18 Point 146

[8] Case C-311/18 Point 141

[9] Case C-311/18 Point 139

## KEY CONTACTS

**CLAUDE-ÉTIENNE ARMINGAUD**
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM