The Schrems II judgment of the ECJ: Consequences for the practice of using standard data protection clauses

Dr. Carlo Piltz, 21.7.2020

Content

A. Systematics of the judgment 1
B. Uniform level of protection for Chapter V of the GDPR 2
C. Requirements for data transfers without an adequacy decision 2
D. Level of protection when using SCC 3
E. Assessment of the currently applicable SCC (2010/87/EU) 3
F. Obligations of the controller (exporter) and the processor (importer) 4
1. The scope of the controller's verification duties 4
2. Content of the obligation 5
3. Implementation in practice? 6

What are the consequences of the Schrems II judgment of the ECJ (C-311/18)? What should be taken into account when transferring data to the US and other third countries? Of course, many companies are currently asking these questions. I do not claim to provide conclusive answers to these questions.

However, in this article, I would like to try to systematically classify the judgement and to "unravel" it a bit. On the other hand, I would also like to deduce possible (!) practical consequences for data controllers and processors. This article therefore concerns the aspects of the ECJ decision referring to the standard contractual clauses (under GDPR: standard data protection clauses; but I will refer to “SCC”). In my opinion, it goes without saying that other interpretations of the judgement are certainly justifiable.

I deliberately refrain from explaining what the background of the proceedings was and also from explaining what the EU US Privacy Shield or the SCC are.

A. Systematics of the judgment

In my opinion, it is appropriate to first take a look at the structure of the ECJ decision. This is relevant because of the length of the judgment. It is easy to get lost in the reasons, only to ask the question of what is actually being examined. I have drawn up a brief outline of this:

1. Level of protection required by Article 46(1) and Article 46(2)(c) of the GDPR in respect of a transfer of personal data to a third country based on SCC? (from margin no. 90)
2. Obligation of the data protection authority to suspend transfers based on those clauses if they are not or cannot be complied with in that third country? (from margin no. 106)
3. Validity of the SCC decision in the light of Articles 7, 8 and 47 of the Charter (“adequate level of protection”)? (from margin no. 122)
4. Whether and to what extent findings in the Privacy Shield decision are binding on the supervisory authority of a member state // whether the transfer of personal data to the US pursuant to the clauses in the annex to the SCC decision breaches the rights enshrined in Articles 7, 8 and 47 of the Charter? (from margin no. 150)
    a. On the content of the Privacy Shield decision (from margin no. 163)

b. To determine an adequate level of protection (from margin no. 168)

B. Uniform level of protection for Chapter V of the GDPR

It is already clear from the outline that the ECJ in the judgement first examines what level of protection is to be achieved at all when data are transferred on the basis of Art. 46 GDPR. In the examination in the first section, the ECJ deals in general terms with the question of what level of protection "appropriate safeguards" must be achieve.

This leads to the abstract question: is there a difference in the level of protection to be achieved by the transfer mechanisms under Chapter V GDPR?

No. According to the ECJ, a uniform level of protection applies to the entire GDPR and thus also to Chapter V. This means that the "appropriate safeguards" referred to in Art. 46 (1) GDPR must be capable of ensuring that data subjects whose personal data are transferred to a third country pursuant to SCC are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially **equivalent** to that guaranteed within the European Union (from margin no. 96).

Margin no. 90-105 do not specifically deal with the currently applicable SCCs, but with this transfer instrument in general. The ECJ considers the general standard of review to be applied to data transfers under Art. 46 GDPR for which the SCCs are an example.

C. Requirements for data transfers without an adequacy decision

According to the ECJ (and the requirements in Art. 46 (1) GDPR), in the absence of an adequacy decision, personal data may be transferred to a third country if the exporter achieves the following three objectives:

- he has provided for "**appropriate safeguards**" (these can be, inter alia, contained in the SCC)
- "**enforceable data subject rights**", and
- "**effective legal remedies for data subjects**" are available (margin no. 91)

These are, for Art. 46 GDPR, the three relevant criteria of the adequate level of protection.

Important: within the framework of Art. 46 GDPR (and thus also the SCC), however, the country of destination and the legal system there does not have to provide an equivalent level of protection. Rather, the "appropriate safeguards" themselves, e.g. the SCC, should guarantee a level of protection for persons that is essentially equivalent to the level of protection guaranteed in the Union (margin no. 96).

This also means that the standard for assessing the level of protection is different in substance from that applied in the case of the adequacy decision under Art. 45 GDPR (see also margin no. 129 and 130). However, the objective to be achieved (essentially equivalence) is the same.

My illustration: in the case of the adequacy finding, the entire third country is a beautiful green data protection area. In the case of Art. 46 GDPR (i.e. the use of SCCs), however, the third country is an evil volcanic landscape in which data is not secure, and with the SCCs we now want to create a tunnel to a specific recipient in that country. There is therefore, as a precondition, a lack of data protection, which must be compensated for by the tunnel for a transfer (see also margin no. 95). This tunnel

must protect the data against the volcanic landscape in accordance with the requirements of Art. 46 GDPR.

D. Level of protection when using SCC

The national court also asked the ECJ which specific factors should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred pursuant to the SCC (margin no. 102).

The ECJ's answer to this question is not very specific and practical. It is, of course, based on the level of protection for Art. 46 GDPR set out above. However, with regards to the three criteria already mentioned above, the ECJ also explains in margin no. 104 that the following points must be taken into account with regard to a transfer based on the SCC:

- in particular, the **contractual clauses** agreed between the controller established in the European Union and the recipient of the transfer established in the third country concerned and
- as regards any **access by the public authorities** of that third country to the personal data transferred, the **relevant aspects of the legal system** of that third country.

And here the ECJ makes an important comparative turn on the conditions for an adequacy decision: as regards access to the personal data transmitted by authorities of the third country, the elements to be taken into account in the context of Article 46 GDPR are the same as those listed, in a non-exhaustive manner, in Article 45 (2) GDPR.

E. Assessment of the currently applicable SCC (2010/87/EU)

Do the currently applicable SCCs meet these requirements? And what exactly has to be considered when using them? The currently applicable SCC (or more precisely, the underlying commission decision) is dealt with by the ECJ from margin no. 122 onwards.

The first important finding of the ECJ is that there may be situations in which the SCCs can be used unchanged, as they themselves provide the appropriate level of protection. The ECJ distinguishes between two scenarios (margin no. 126):

- Scenario 1: Depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data **solely on the basis of SCC**.
- Scenario 2: Situations in which the content of those standard clauses might not constitute a **sufficient means** of ensuring, in practice, the effective protection of personal data transferred to the third country concerned.

As regards scenario 2, the Court gives an example: where the law of that third country **allows** its public authorities to **interfere with the rights of the data subjects** to which that data relates.

Note: just because interference with the rights of data subjects is possible and cannot be excluded by the non-adapted form of the SCC, the SCC are not inappropriate. I think it is important to recognize this.

This is because, according to the ECJ, Art. 46 (2) GDPR does not require that all safeguards are necessarily provided for in a Commission decision such as the SCC decision (margin no. 128). This is

not even possible, as the SCC are only drafted in general terms and apply to all third countries (margin no. 130, 133).

From margin no. 137 onwards, the ECJ then deals with the Commission's decision on the currently applicable SCCs. The comments are thus of a rather abstractly evaluative nature. However, in its examination of the validity of the decision, the ECJ also deals with obligations that apply to those who are responsible and explains how these obligations are to be fulfilled.

F. Obligations of the controller (exporter) and the processor (importer)

And now we are also approaching practical guidelines. According to the ECJ, due to the general nature of the SCC, in the above-mentioned scenario 2, depending on the situation in a given third country, the adoption of **supplementary measures** by the controller in order to ensure compliance with that **level of protection** may be necessary (margin no. 133).

Once again, it should be recalled that the ECJ has ruled that the level of protection of SCC is equivalent to that in the EU.

And the ECJ goes even further: it is above all, for that controller or processor **to verify**, on **a case-by-case basis** and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination **ensures adequate protection, under EU law**, of personal data transferred pursuant to SCC, by providing, where necessary, **additional safeguards** to those offered by the SCC (margin no. 134).

Attention: this means that the exporting controller must at least validate, before the transfer, whether the unmodified form of the SCC can be used to maintain the level of protection (which they create per se). This validation does not concern the complete law of the third country. The ECJ clearly refers to the specifically transferred data: "… *ensures adequate protection, under EU law, of **personal data transferred pursuant to standard data protection clauses …***" (margin no. 134). Moreover, an examination of the entire legal system would not be compatible with the ECJ's previous reasoning on the difference between the adequacy finding and the SCC.

If the exporter or the recipient of the data is not able to take adequate additional measures to comply with the SCC standard, he is required to suspend or end the transfer of personal data to the third country concerned (margin no. 135). The ECJ also cites an example: “Where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to the SCC and are, therefore, capable of impinging on the contractual guarantee.”

1. The scope of the controller's verification duties

And the question then naturally arises as to what specifically the controller has to verify before the transfer of data? Is it enough for the importer to prove that he can comply with the SCC? Does the controller have to carry out his own investigations?

According to the ECJ (margin no. 141), the answer to this question can be found in the clauses of the SCC, specifically in Clause 4 (a) and Clause 5 (a) and (b). These oblige the controller established in the European Union and the recipient of personal data **to satisfy themselves** that the legislation of the third country of destination enables the recipient to **comply with** the standard data protection clauses in the annex to **the SCC decision, before transferring personal data to that third country**.

This means that the verification question here, at the first stage, is: can the recipient comply with the SCC on the basis of the law applicable to him?

This directly leads to some valuable insights:

- It is always about the specific transfer based on the SCC; not generally about transfers to the third country.
- This means that compliance with the SCC must always be checked on a contract-specific basis.
- Compliance with the SCC with regards to the law in the third country must therefore probably also be checked specifically on the basis of the data to be transferred and the specific recipient (and not generally).
- Both the data controller and the recipient are obliged to make sure that they comply with the SCC (of course, especially in the form of cooperation).

2. Content of the obligation

And the ECJ also gives an indication as to what the contracting parties must take into account as evaluation criteria in this examination, so what they need to "verify".

The footnote to Clause 5 of the SCC makes it clear that mandatory requirements of law in the third country which do not go beyond what is necessary in a democratic society to ensure, inter alia, state security, defense and public safety, do not contradict the SCC.

In other words, an adequate level of protection may also exist on the basis of the SCC if authorities of the third country access the data transferred. This is an important clarification by the ECJ that is also relevant in practice.

However, this access must be legislatively structured in such a way that it meets the requirements of the former Art. 13 (1) of Directive 95/46/EC. There, objectives were listed which restrictive legislative measures must pursue in order to be permissible.

Art. 13 Directive 95/46/EC no longer exists, however. Since, according to Art. 94 (2) GDPR, references to Directive 95/46/EC are to be understood as references to the GDPR, I believe that Art. 23 (1) GDPR and the objectives listed therein (which are very similar to those of Art. 13 (1) Directive 95/46/EC) must now be replaced by Art. 23 (1) GDPR. These include:

- national security;
- national defense;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of sentences, including the protection against and prevention of threats to public security
- the protection of the independence of the judiciary and the protection of court proceedings;
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

But: it is not enough that the law of the third country pursues such an objective when accessing the data. Access must also be necessary to pursue that objective. A proportionality test is therefore required. And here I think it will be very difficult for European companies alone to carry out this test in a valid way. The recipients in the third country should therefore provide support in this respect.

The ECJ emphasizes that it is to be regarded as an infringement of the SCC if an obligation arising from the law of the third country of destination is fulfilled which goes beyond what is necessary for purposes such as those mentioned above.

3. Implementation in practice?

In practice, the controller could, for example, use a pre-prepared questionnaire to validate whether access is possible and if so, for what purpose. If access to the data is possible, this access must be checked for its necessity. In my opinion, it does not follow from the judgment that the controller must carry out this check himself. It should also be okay if the importer can prove to the controller (for example by means of a legal opinion) that the access by authorities meets the European requirements.

The verification test is therefore roughly structured as follows:

Step 1: Use of the unchanged SCC. Can the recipient comply with all SCC obligations?

- The controller must "verify" this (if necessary, in cooperation with the recipient).
- "Verify" includes checking whether the data can be accessed by authorities.
- If so, then it must be assessed whether the accesses are necessary and required to serve a purpose mentioned in Article 23 (1) GDPR.

Step 2: SCC obligations alone are not sufficient. Additional measures must be implemented (margin no. 146).

- These measures may be of a contractual or technical nature.
- Caution: Risk for the importer to violate national law.

In my view, it is important to make it clear once again that the ECJ considers that the lack of possibility to comply with the SCC obligations does not directly lead to the inadmissibility of the transfer. Only if additional means or safeguards do not help, the transfer must be prohibited by the supervisory authority or by the exporter beforehand. This follows from margin no. 146: "... those 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** …".

The ECJ then concludes in margin no. 149 by stating that the SCC in its current version and through the safeguards contained therein basically provide the required level of protection (margin no. 96, "essentially equivalent"). If compliance with the SCC is not possible, one would have to continue with the above-mentioned step 2 of the examination and implementation of further safeguards.