Checklist for transferring personal data after schrems II

TIMELEX

The CJEU ruling from 16 July 2020 in the Schrems II case created a lot of uncertainty for organisations transferring personal data outside the EEA. Not only was the EU-US Privacy Shield invalidated, the Court also imposed conditions for the use of standard contractual clauses (SCCs) as a mechanism to transfer personal data to non-EEA countries and this without any grace period. Any such transfer must at all times provide adequate safeguards to ensure a level of protection essentially equivalent to that provided by EU law.

But how should this requirement be fulfilled in practice? Can the EEA-based party be expected to scrutinise all foreign law systems and decide whether additional legal safeguards are needed on a case-by-case basis? And which measures should it take? How should it provide adequate protection against access by public authorities in the non-EEA countries? How should it ensure that data subjects' rights or remedies are at all times respected?

Both the European Data Protection Board (EDPB) and the European Commission came up with some first practical guidance and instruments on 11 and 12 November respectively.

1. The EDPB Guidance of 11 November 2020

The EDPB actually issued **two sets of recommendations.**

First set

[Recommendations on supplementary measures for transfer tools]

Status: draft

Organisations can provide feedback until 30 November 2020.

This set contains the draft supplementary measures recommended by the EDPB to make international transfers permitted under the GDPR.

The EDPB proposes to follow a roadmap with six logical and sensible steps (as such confirming what some organisations had already been doing since the Schrems II-ruling):

Step 1. Know your transfers.

> e.g. assess necessity, ensure data minimisation, etc. This requires a proper data mapping exercise. Are there onward transfers?

Step 2. Verify the transfer tools you are relying on.

> Article 45 to 49 GDPR.

> only EC adequacy decisions offer 100% certainty.

Step 3. Assess the effectiveness thereof in the context of the law or practice of the third country.

> for this assessment the second set of EDPB recommendations will be useful as well as certain academic initiatives, such as this one.

>ask the data importer to provide information on legislation, case law and jurisprudence in the third country.

Step 4. Identify and adopt supplementary measures in view of reaching equivalent protection.

> can be technical (e.g encryption), organisational (e.g. internal policies) or legal (e.g. contracts) measures.

> don't transfer if supplementary measures appear insufficient.

Step 5. Take formal procedural steps to fulfil the fourth step if necessary.

> contact the competent supervisory authority if needed under article 45 or 46 GDPR.

Step 6. Assess your supplementary measures on a regular basis.

Second set	Recommendations on European Essential Guarantees for surveillance measures Status: final	This set provides guidance on how to assess the effectiveness of the transfer tool **in the context of the law or practice of the third country**.

2. The draft SCCs of 12 November 2020

The European Commission published the long awaited new SCCs pursuant to the GDPR together with the draft implementing decision for these SCCs.

As expected, the new SCCs take a modular approach to be used in **4 scenarios**:

(i) controller-to-controller transfers;

(ii) controller-to-processor transfers;

(iii) processor-to-processor transfers; and

(iv) processor-to-controller transfers.

The new SCCs require data exporters to perform a **data transfer impact assessment** (TIA). Hence, such a TIA is now a formal requirement and no longer based on EDPB guidance only.

Sub-processors would have to accept audits from the EEA-based controller. As there may be a very large number of controllers relying on the same sub-processor, it will be interesting to see how sub-processors will react to such a requirement.

There remains a difference between non-EEA based organisations who are directly and fully subject to the GDPR and those who are contractually bound to follow its principles based on the SCCs.

The new SCCs are still in draft form. Organisations can **provide feedback** until 10 December 2020. Adoption of the final SCCs is expected early 2021.

3. Our assessment and main takeaways

1. Use the opportunity to provide feedback

We would encourage organisations to use the opportunity given to provide feedback on the first set of EDPB recommendations and on the draft SCCs until 30 November 2020 and 10 December

2020 respectively.

2. Need to act now and document your approach

The supervisory authorities will enforce the new requirements and there is no indication that they will postpone their actions. Hence, a wait-and-see approach is no option. Organisations should start their data mapping exercise and data transfer impact assessment as soon as possible. This should allow them to reach first conclusions on whether supplementary protection measures are needed and what they should look like. All efforts in this respect should be properly documented as part of the overall accountability obligation under the GDPR.

3. The EDPB recommendations are not ready-to-use

The EDPB recommendations are quite generic in nature and recommend the same measures for all types of personal data, without taking into account the nature of the data. This is regrettable from a proportionality point of view. Hence, organisations should still make this assessment for themselves.

4. The draft SCCs are complex and detailed, offering more possibilities

The new SCCs offer more possibilities. EEA-based controllers and processors can select the module that suits them best and can incorporate the clauses in to a larger agreement. The EDPB guidance should be taken into account in order to supplement the SCCs where appropriate and required. Additional contractual measures could, for example, include obligations to inform the EEA-based exporter of any access and disclosure requests in the third country and to obtain a waiver where possible.

There is a one-year sunset period to repeal any current SCCs in use. Although the new SCCs will not be formally adopted before early 2021, we recommend organisations who transfer a lot of personal data, especially when such data are sensitive, to start with their TIA already.

In case of a no-deal Brexit by the end of the transition period on 31 December 2020, EEA-based organisations would have to put in place the current SCCs as of 1 January 2021 with respect to UK data importers and replace them by the new SCCs some months later.

5. Technical measures can help reach adequate protection but won't necessarily do so

Encryption and pseudonymisation may be used but only if their use truly offers effective and adequate protection. Encryption must be very strong and done in such a way that the data cannot be decrypted in the third country, even if data at rest is fully encrypted. Hence, the data importer may not be involved in any way in key management. This means that the EEA-based data exporters must make sure that the applied pseudonymisation makes any re-identification of the data subject in the third country impossible. This may prove to be a very difficult obligation.

Authors: Geert Somers, Liesa Boghaert