Luther.

Newsflash | 20.11.2020

“Schrems II” compliance: what next?

The past week was one of the busiest weeks for data protection practitioners since the EU General Data Protection Regulation came into effect. On Tuesday, 10 November, the European Data Protection Board (EDPB) adopted recommendations as to the possible form of the additional measures of protection that should be taken when transferring data on the basis of standard contractual clauses to third countries which do not have an adequate level of data protection. On Thursday, 12 November, the European Commission published the long announced draft standard contractual clauses.

In a nutshell:

- **The first European interpretation guide following the “Schrems II” decision has been published.**
- **The EDPB and the national supervisory authorities are specifically focusing on the transfer of unencrypted data to cloud service providers, amongst others.**
- **New standard contractual clauses have been presented in draft form and are expected to be adopted in early 2021.**
- **The time allowed to transition to the new standard contractual clauses will be one year.**

What has happened so far?

In July, the European Court of Justice issued its “Schrems II” decision (C-311/18), in which it (i) declared the “Privacy Shield” between the EU and the USA to be invalid and (ii) decided that organisations can, under certain circumstances, continue to rely on the standard contractual clauses (SCCs) to transfer personal data from the European Economic Area (EEA) to the USA or another country which, in the opinion of the EU, does not have an adequate level of data protection. However, in order to be able to rely on the SCCs when making such transfers, the company transferring the data must assess on a case-by-case basis whether the laws of the third country

offer an "essentially equivalent" level of protection for the personal data and, if necessary, adopt "supplementary measures" to ensure such protection. The data protection supervisory authorities in the various Member States of the EU have published varying announcements regarding the enforcement of this decision. Accordingly, we had developed a provisional first-aid kit that can be used to evaluate data transfers and identify and address risks; this package has partly anticipated the EDPB recommendations.

What is new?

The EDPB recommendations now provide a European interpretation guide for data transfers following the Schrems II decision. At the same time, the European Commission has presented a draft version of the new standard contractual clauses. These new SCCs differ significantly from the SCCs that have applied until now. Perhaps the most exciting development is that the draft SCCs are structured as "modules" that cover transfers in all conceivable constellations, including now also transfers between two data processors. The "module" to be used for transfers from controller to data processor meets the requirements under Article 28 GDPR, which means that a separate processing agreement will no longer be required.

These developments pose various challenges to companies.

- SCCs that have already been concluded, or are about to be concluded, must be supplemented with additional measures, according to the EDPB recommendations, if the laws or any other practice in the third country might impair the effectiveness of the adequate safeguards, such as the SCCs. If the company assessing this issue arrives at the conclusion that the third country's legislation permits surveillance measures which impair the effectiveness of the SCCs, additional measures will have to be taken. Assessing whether the data that is to be transferred in the individual case would be affected by the surveillance legislation is particularly difficult in practice.

  The EDPB has identified various transfer constellations and described, by way of an example, which additional technical and/or contractual measures could be agreed. The 6th group of cases describes the services provided by a cloud service provider who needs to have access to unencrypted data to be able to provide the services. In this case, the EDPB does not see any possible way to enable this transfer to take place in conformity with the law if the outcome of the analysis of the situation in the third country is that a comparable level of data protection cannot be ensured. The same applies correspondingly to access within a group of companies if a group company in a country that does not have an adequate level of personal data protection is intended to be granted access to personal data that is in plain text form. For these groups of cases, the recommendations should probably be understood to mean that transfers continue not to be allowed. Consequently, strong encryption and pseudonymisation as a sufficient measure to ensure that a transfer conforms to the law can only work as long as the data remains continually encrypted and pseudonymised.

- The EDPB recommendations dated 10 November 2020, which state that the SCCs that are currently in use should be supplemented by technical and contractual measures, now need to be assessed in light of the new draft SCCs from 12 November 2020. The currently valid SCCs will become invalid once the Commission's decision on the new SCCs takes effect, albeit at the end of the currently planned one-year transition period. The Commission is authorised to adopt standard contractual clauses by way of an "implementing act" ("examination procedure" pursuant to Article 5 (EU) No. 182/2011). The Commission is required to agree the draft implementing act it is proposing with a committee composed of representatives of the individual Member States of the EU. The proposal must be supported by a qualified majority of the committee. The deadline for comments on the new draft SCCs is 10 December 2020; the new draft SCCs could then, subject to further amendments, probably take effect in 2021.

- The EDPB recommendations are partly reflected in the new standard contractual clauses. This relates, in particular, to the question of transparency of access to transferred data by public authorities and the requirement to exhaust all legal remedies against such access and keep statistics about the access. In part, however, the new SCCs take into account to a greater extent than the requirements of the EDPB the data importer's interests and the legal requirements that the data importer is subject to in its country. The contractual safeguards are fully formulated in the new SCCs; by contrast, the SCCs do not contain any specific rules on the technical measures to ensure security and confidentiality. In this respect, the EDPB recommendations remain relevant. The recommendations on supplementary measures for transfers are subject to consultation until 30 November.

What needs to be done?

The relevant transfers to third countries should be identified, to the extent this has not already been done. The EDPB now requires, in particular, that an examination be carried out to verify whether the level of protection of personal data in the data recipient's country is adequate. The next step should then be to examine technical measures of protection on the basis of the scenarios established by the EDPB for whether they can be used in the current constellation. Only when the general suitability of such technical measures has been established can additional, contractual measures be considered. The examples given in the EDPB recommendations can be used as a guideline here; on the other hand, they can also be interpreted in light of the new standard contractual clauses. It transpires in this context that the EDPB's considerations have, to a certain extent, been taken into account in the new draft SCCs; however, the coordination between EDPB and Commission was not seamless enough for the contractual safeguards that are required by the EDPB to be included on a 1:1 basis in the standard contractual clauses. In light of this, the question rightly arises as to whether the new standard contractual clauses would also have to be supplemented by far-reaching measures of protection and whether the wording of the new SCCs relating to government access provides a solution that is already practicable now. It is very unlikely that the EDPB will withdraw its requirements upon expiry of the deadline for comments and amend its recommendations in this regard.

Consequently, companies should now supplement the currently applicable SCCs taking these requirements into account and should also, at the same time, integrate an "opening clause" that will make it easier for them in the future to make amendments and changes to their contracts once the new SCCs have been adopted. The work on the technical measures of protection and the development of verifiable approval processes should be preparatory work in this regard that will endure once the new SCCs take effect. This work will, however, continue to be a provisional arrangement and will need to be followed by the appropriate contractual amendments.

Recommended course of action:

- Identify international data transfers;
- Amend the technical and organisational measures to ensure that they comply with the EDPB recommendations; examine whether access to unencrypted data in the third country is absolutely necessary;
- If unencrypted data is being processed, verify whether the service provider and the services concerned are subject to surveillance legislation;
- Supplement any existing SCCs in line with the EDPB recommendations and the new SCCs and include an "opening clause" in the SCCs that will make it possible to transition to the new SCCs in 2021; and
- Start to plan the project to transition to the SCCs in 2021.

Timeline

Now
Identifying international data transfers

Subsequently
Agreeing additional safeguards for insecure transfer contexts

Ca. 1/2021 to 1/2022
Project to implement new SCCs

Contacts:

Dr Jörg Alshut

Berlin

T +49 30 52133 21890

joerg.alshut@luther-lawfirm.com

Silvia C. Bauer

Cologne

T +49 221 9937 25789

silvia.c.bauer@luther-lawfirm.com

Dr Maximilian Dorndorf

Essen

T +49 201 9220 24027

maximilian.dorndorf@luther-lawfirm.com

Dr Stefanie Hellmich, LL.M.

Frankfurt a.M.

T +49 69 27229 24118

stefanie.hellmich@luther-lawfirm.com

Dr Kay Oelschlägel

Hamburg

T +49 40 18067 12175

kay.oelschlaegel@luther-lawfirm.com

Christian Kuß, LL.M.

Cologne

T +49 221 9937 25686

christian.kuss@luther-lawfirm.com

Dr Michael Rath

Cologne

T +49 221 9937 25795

michael.rath@luther-lawfirm.com

Carsten Andreas Senze

Stuttgart

T +49 711 9338 25222

carsten.a.senze@luther-lawfirm.com

Dr Wulff-Axel Schmidt

Frankfurt a.M.

T +49 69 27229 27078

wulff-axel.schmidt@luther-lawfirm.com