European Commission
European Data Protection Board

abbreviation RR
+Tel. 14952
+Fax. 514952
Vienna, 04. Dezember 2020

Recommendations 01/2020, 02/2020 und standard contractual clauses

Dear ladies and gentlemen,

we very much welcome the speed with which guidelines for international data transfer (iDT) as well as recommendation 02/2020 were drawn up and the standard contract clauses (SCC) were revised following the Schrems II findings.

- **ad Recommendations 01/2020 on measure that supplement transfer tools on ensure compliance with the EU level of protection of personal data**

The document leaves open the question of which of the additional measures mentioned are capable of establishing a legally compliant state and thus legal certainty. This against the background that especially the transfer to the USA and in this context FISA 702 and Executive Order 12333 are presented as a major problem. It is also doubtful that the repeatedly cited encryption by the data exporter can be regarded as a "panacea", as the regulation of the 50 USC § 1881a (FISA 702) requires a release of the key, which means that the data may not be personal to the data importer himself because it is encrypted, but the key may have to be released to the authorities. In this context, it should be noted that the statements in paragraphs 52 and 76 are contradictory, although it is rather assumed that this is an editorial mistake and that encryption - as described in Use Case 1 - is a suitable technical measure.

On the other hand, supplementary contractual measures are largely regarded as insufficient. However, considering that (end-to-end) encryption or pseudonymization of all data in international data traffic is difficult to imagine, if not impossible, this would make the use of standard contractual clauses, such as those provided by the GDPR

itself in Art. 46, largely obsolete. But these have just been revised by the European Commission.

It would therefore be desirable to revise the document with a view to a risk-based approach, as provided for not only by the - newly revised standard contractual clauses, but by the GDPR itself. Likewise, as will be shown, companies will be overburdened with "test requirements", which even large companies will find difficult to cope with. It would therefore also be desirable if it were possible in individual cases to consult the supervisory authority in advance in order to establish legal certainty, at least for the time being.

The structure and principle of the 6-step plan set out in the document is absolutely welcome. Step 3, however, involves examining the "law of the third country that may impinge on the effectiveness of the appropriate safeguards". Even if this was to be expected on the basis of the ECJ ruling, it is a challenge for companies that will be difficult or impossible to overcome. It also remains unclear, for example, what is meant by "possible sources of information". It is not acceptable that a possible examination of compliance with the GDPR regulations should also include "sources" that lie outside of publicly available legal acts or "state" decisions.

According to Art. 45 GDPR, the Commission may adopt an adequacy decision declaring that the level of protection in a third country is guaranteed. Since it can be assumed that the Commission uses checklists, questionnaires or similar when examining the level of protection in a third country and since these decisions are not based on chance, it would be far more efficient and useful if these checklists, questionnaires or similar could be made available to companies. However, it would be even more efficient in terms of the competitiveness of the European economy if this were to be carried out by the European Commission as part of the examination of the level of protection, by the EDPB or a similar central EU body and published in a database - whether this is only to be made available after registration or is generally accessible. Otherwise, companies within the EU would not only invest a great deal of time, but above all a great deal of money to check the level of protection, unless there is an adequacy decision. And that cannot be in the EU's interest.

In step 4, contractual measures are proposed, but these are more or less immediately presented as ineffective in relation to data access by the authorities. However, if - additional - contractual measures are called into question, the standard contractual clauses are also put into contracts at the same time, which however, especially in the revised version, seem to be quite capable of establishing an adequate level of protection.

- **Recommendations 02/2020 on the European Essential Guarantees for surveillance measures**

The EEG must also be taken into account in the examination according to Recommendations 01/2020. These also provide for a comprehensive examination of the legal framework in the third country, which is why reference is made to the above-mentioned explanations. It also raises the question of when a regulation is "clear and precise" in the sense of the EEG and whether it is "necessary and proportionate". This leaves the companies completely alone, because they have to make decisions here whose correctness will only be determined by the ECJ. Even if the companies will not be completely relieved of the risk, it would still be helpful to have the relevant guidelines of the EDPB or a corresponding database available.

- **Standard Contractual Clauses**

The revision and especially the "modular design" are to be emphasized positively. In particular, the "risk-based approach" chosen here and clauses such as those in the information duties (keyword: "as far and as much as possible" in the information duties) are to be regarded as quite achievable. However, in view of the fact that the previous standard contract clauses do not contain all the conditions listed in Art 28 GDPR that must be included in a corresponding contract, but the revised version does, it would be desirable to clarify in the SCC that an agreement in accordance with Art 28 GDPR is also given when the contract is concluded.

With kind regards

Rainer Rauch
Dataprotection Officer