alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS

The new Standard Contractual Clauses of the EU

Antonia Herfurth, Attorney at law in Munich and Hanover

May 2022

On June 4, 2021, the European Commission issued new Standard Contractual Clauses (SCCs) for international data transfers.[1] The new SCCs are an adaptation to the General Data Protection Regulation, which came into force in 2018. Since September 27, 2021, new data transfer contracts and contract amendments may only be concluded using the new SCCs. By December 27, 2022, all old contracts must be adapted to the new SCCs. The old SCCs, which were still based on the Data Protection Directive 95/46/EC from 1995 and were up to 17 years old, have been replaced. If the old SCCs are continued to be used, the transfer of data can be prohibited and a fine can be imposed.

With the new SCCs, the Commission hopes for more legal certainty and flexibility in data transfers to third countries. For the parties, however, the data transfer will also become more complicated.

Overview

The processing of personal data must always be based on a legal basis, such as the consent of the data subject. If personal data are transferred to non-EU countries (third countries), this requires a further legal basis. If data crosses borders within the EU, the transfer is always permissible because the data protection level of the GDPR applies. Cross-border transfers to third countries where the GDPR does not apply, but on which the Commission has reached an adequacy decision, are also permissible. According to the Commission, they have an adequate level of data protection comparable to that of the GDPR and are considered "safe third countries" (e.g. Canada, Japan, UK). Third countries for which there is no adequacy decision are classified as "unsafe third countries". The transfer of personal data is only permitted if the controller or processor has provided appropriate safeguards, these include SCCs. SCCs are model contracts approved by the Commission.

Structure

The new SCCs for the transfer of personal data to third countries consist of one document with a modular structure. The four modules cover different transfer scenarios. Section I of the SCCs (e.g. "Purpose and Scope", "Effect and Invariability of the Clauses"), Section III ("Local laws and practices affecting compliance with the Clauses") and Section IV ("Final provisions") are essentially applicable to all modules. The new SCCs

[1] The new SCCs are available under https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

include clauses on liability, applicable law and jurisdiction.

While the old SCCs only covered two scenarios, the new SCCs cover the following data transfer scenarios:

Module 1: C2C

Module 1 covers the transfer of data from a controller in the EU to a controller in a third country (*Controller to Controller*). The old SCCs already covered this situation.

Module 2: C2P

Module 2 covers the transfer of data from a controller in the EU to a processor in a third country (*Controller to Processor*). This situation was also covered by the old SCCs. However, the new SCCs have the advantage that controllers no longer have to conclude a separate processing agreement with processors in a third country. According to Article 28 of the GDPR, the processing of data by a processor may only take place on the basis of a (processing) agreement. Module 2 now covers this requirement.

Module 3: P2P

Module 3 covers the situation where a processor in the EU transfers data to a (sub-)processor in a third country (*Processor to Processor*). Processors in the EU can therefore use sub-processors outside the EU. This constellation was newly introduced. If a processor wanted to use a sub-processor under the old SCCs, it was necessary for the controller itself to conclude SCCs with the sub-processor. The processor could not independently use a sub-processor even though there was a processing agreement between the processor and the controller. This has now changed. Module 3 is similar to Module 2, with the consequence that parties no longer need to conclude a separate (sub-)processing agreement. This reduces the organisational burden on the controller.

Module 4: P2C

The scenario under Module 4 is also new and covers the (re-)transmission of data from a processor in the EU to a controller in a third country (*Processor to Controller*). Unlike Modules 2 and 3, Module 4 does not meet the requirements of Article 28 of the GDPR, i.e. separate data processing agreements must be concluded.

Individual questions regarding this module and its relevance for practice are discussed. For example, some data protection experts have commented that it feels “strange” that the processor is subject to the instructions of a controller located in a third country where the GDPR does not apply.

Use

The SCCs can be concluded as an individual contract or as part of a comprehensive contract. Like the old SCCs, they may not be changed. If the SCCs are changed, they are null and void. In particular, as part of a comprehensive contract, no further clauses may be included which contradict the SCCs or impair the fundamental rights or freedoms of the person concerned. If contractual or GTC clauses contradict the SCCs, the SCCs take precedence. However, the SCCs need to be supplemented in some parts. In Article 17, the parties must specify which Member State's law should apply to the SCCs, and in Module 3, the parties can choose between two options. In Article 18, the parties have to indicate which Member State's court should be competent. Furthermore, the Annex has to be filled in with information on the contracting parties, a description of the data transfer, etc.

Article 7 introduces an optional docking clause. According to this clause, an entity that is not a party to the SCCs may join them at any time with the consent of the contracting parties. The accession is done by filling in the Annex and signing Annex I.A. of the Implementing Decision (EU) 2021/914 which introduced the new SCCs. The docking clause allows for the accelerated accession of third parties, i.e. more flexibility.

Newly introduced obligations

As a result of the CJEU's Schrems II ruling in 2020, the SCCs introduce new obligations for data exporters and data importers. "Data exporter" means the person, authority, agency and other body in the EU that transfers personal data to a third country. "Data importer" means the entity in a third country that receives personal data.

Mandatory Transfer Impact Assessment

The new SCCs oblige data exporters and importers to verify whether the third country has a level of data protection that complies with the GDPR. In addition, the likelihood of third country authorities accessing the data can be taken into account. This so-called Transfer Impact Assessment (TIA) must be carried out for each individual data transfer. If the third country does not have an adequate level of data protection, the data exporter must attempt to achieve this level through additional technical security measures. Since both the assessment of third countries and the identification of appropriate additional measures are complex, the European Data Protection Committee (EDSA) adopted Recommendations on June 18, 2021, to assist both parties in six steps.[2] If local rules and practices mean that the SCCs cannot be definitively complied with, the data exporter may not transfer personal data to the third country. The SCCs do not bridge this gap. Data importers must provide the data exporter with relevant information for the assessment. If they have reason to believe that the level of protection is changing, they must notify the data exporters without delay.

Obligations to ensure the level of protection

If the data exporter has reason to believe that the data importer in the third country can no longer comply with the level of data protection, he must remedy the situation without delay. To this end, the data exporter must take appropriate measures, such as technical and organisational measures to ensure security and confidentiality, so-called TOMs. The EDSA has listed concrete examples of suitable TOMs in Annex 2 of its Recommendation. If the level of data protection cannot be maintained, the data exporter must suspend the data transfer. In this case, he is entitled to terminate the data transfer contract.

The data importer has a duty to notify if an authority requests him to disclose personal data. If the data importer is prohibited from notifying the data exporter and, if applicable, the data subject, due to the regulations of the third country, he must endeavour to have the prohibition on notification lifted. In addition, the data importer must check the legality of the official disclosure request and, if necessary, challenge it.

Extensive documentation obligations

Both the data exporter and the data importer are subject to extensive documentation obligations. For example, the TIA and all documents relating to official requests for the disclosure of personal data must be documented. The information must be made available to the competent data protection authority upon request.

Data transfers to the USA, China and Brazil

Currently, data transfers to the USA, China and Brazil are only permitted on the basis of SCCs. However, after the CJEU annulled both the Safe Harbor Agreement and the Privacy Shield, the EU and the USA are seeking a new agreement for data transfers. Brazil and China have enacted new data protection laws that came into force in 2020 and 2021 respectively. Although both laws are intended to establish a strong level of data protection, the EU still considers both countries to be insecure third countries. However, the data protection laws can be taken into account in the TIA.

[2] The Recommendations of the EDSA are available under https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

Recommendation for action

New contracts may only be concluded using the new SCCs, old contracts must be adapted by December 27, 2022. The following steps are recommended to ensure that data transfers to third countries continue to be GDPR compliant. The steps should be implemented as early as possible, as they can be extremely time-consuming:

1. Identification of existing contracts and adaptation to new SCCs.
2. Conclusion of new contracts only with the use of new SCCs.
3. Checking the legal situation and practice of the third country, i.e. carrying out a TIA. No data transfer to a third country without ensuring a level of data protection that complies with the GDPR.
4. Documentation of correspondence, measures, considerations, etc.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Alisha Daley-Stehr, Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	++-(0) 511-307 56-20
Fax	++-(0) 511-307 56-21

Alliuris in Germany

Firm	Herfurth & Partner Luisentraße 5, D-30159 Hanover
Web	www.herfurth.de
Fon	+ 49 511 30756 0
Fax	+ 49 511 30756 10
Mob	
Contact	Ulrich Herfurth, Partner
Languages	German, English, French, Spanish, Portuguese, Russian, Mandarin, Czech, Polish
Mail	info@herfurth.de

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt