Global data transfer: The new standard data protection clauses - What needs to be done?

THE EU COMMISSION HAS ADOPTED NEW STANDARD DATA PROTECTION CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES.

Executive summary

- On 4 June 2021, the EU Commission adopted new standard data protection clauses (also called standard contractual clauses (SCCs)).
- This fundamental revision to the SCCs was made necessary by the elevated requirements under the EU General Data Protection Regulation (GDPR) as well as the CJEU's Schrems II ruling.
- The new SCCs are more flexible to use and eligible for a wider range of applications.
- Important new developments here include the mandatory impact assessment and notification obligations to data subjects. The requirement to conclude separate data processing agreement will no longer apply in the future.
- There is a transition period. For existing contracts, the new SCCs must be agreed by no later than the end of 2022.

I. Background - Foundation for data transfer to third countries, in particular the USA

The transfer of personal data to a country outside the EU / EEA - i.e. to a third country (in particular to the USA) - is only permissible if, in addition to the general data transfer requirements under the GDPR, it is also ensured that personal data is sufficiently protected by the recipient in a third country. The general and specific requirements laid out in Art. 44 ff. GDPR apply to such end. For implementation in practice, the EU Commission had already adopted so-called standard contractual clauses under the old data protection law in 2010 via Decision 2010/87/EU, the use of which was intended to ensure that all personal data leaving the EU or the EEA would be transferred and processed in line with applicable data protection law. For data transfers to the USA, the EU-US Privacy Shield framework was also available as an alternative. The Privacy Shield featured a mechanism for verifying US companies certified under it as having a level of data protection comparable to the EU in order to legitimise data transfers to the USA.

However, the Schrems II ruling handed down by the Court of Justice of the European Union (CJEU) on 16 July 2020 invalidated data transfers carried out under the EU-US Privacy Shield without providing for a transitional arrangement. From that point on, data transfer to the USA was no longer possible under the Privacy Shield mechanism.

In its ruling, the CJEU left the SCCs fundamentally untouched. However, the Court did clearly state how, beyond the mere use of the SCCs, data exporters would be responsible from then on for verifying the suitability of data protection and data security safeguards in third countries on a case-by-case basis, and also for undertaking complementary measures to close protection gaps and bring the standard up to the level prescribed by the GDPR.

Thus, the Schrems II ruling represented a turning point for data protection requirements in third-country data transfers. In response, the EU Commission was obliged to fundamentally review and revise its SCCs as a whole, such that an adequate level of protection would be in place once again for the transfer of personal data to third

countries. Advancements in the digital economy likewise made revision and adaptation of the SCCs necessary.

II. Higher requirements on data transfers after the Schrems II ruling

According to the CJEU, the permissibility of a data transfer under the former SCCs is conditional upon the contractual provisions being met and the transfer protection requirements under Art. 45 para. 2 of the GDPR actually being accounted for in the third country to a sufficient degree. The CJEU placed a focus on special protection against access to personal data by foreign security authorities. Enforceable rights and effective remedies must be available to data subjects, as specified in Art. 47 of the Charter of Fundamental Rights of the European Union. Data transfer must be suspended or prohibited if the competent supervisory authorities in the EU are of the opinion that the SCCs are not met or cannot be met in the third country.

The former SCCs no longer met those requirements, which became particularly clear in the case of the USA. The requisite EU standard of protection cannot be guaranteed in the USA due to the far-reaching scope for security authorities there to access personal data. To cite one example, security authorities in the USA are able to access personal data without a court order. The possibility of turning to an ombudsman in the USA in order to punish legal violations also is not (or no longer) sufficient to guarantee effective legal protection. According to the CJEU, an ombudsman cannot be equated with an independent judge.

III. Fundamental changes in the new standard data protection clauses

1. Modular structure

Users wield a greater scope of discretion under the new SCCs. The new SCCs offer more flexibility and are eligible for a wider range of applications. Whereas the former SCCs only included provisions on data transfer between two controllers and controller and processor, the following four contractual modules and data transfer use cases are now covered in a more distinguishing manner in addition to the general clauses:

Module 1: Controller to controller
Module 2: Controller to processor
Module 3: Processor to processor
Module 4: Processor to controller

2. Significant changes

Since the former SCCs pre-date the GDPR, the new SCCs have been adapted to align overall with that Regulation's wording and requirements. The most important new developments are as follows:

a. Mandatory impact assessment

One significant innovation in the SCCs is the mandatory data protection impact assessment.

Both parties, the data exporter and the data importer, must declare they have no concerns regarding the data protection standard in the data importer's country. It is particularly important here to critically examine the data protection requirements and safeguards in the third country (country of the data importer) - including the obligations for disclosing personal data to authorities.

The impact assessment must be documented and made available to supervisory authorities upon request.

b. Notification to data subjects

The data importer must notify the data exporter and the data subject when a legally binding order to disclose personal data is received from a public authority. The data importer must also check the legality of a disclosure order of this kind. If the data importer concludes that the request is unlawful, then the data importer must challenge the order, exhausting all available legal remedies as needed.

c. Protection for third parties

With certain exceptions, data subjects themselves can assert their rights against all users of their personal data in the data transfer chain; i.e. also directly against processors.

d. Subsequent accession of further contracting parties possible

In the future, it will be possible for a third party to join as a data importer or exporter after the SCCs have been concluded, provided both parties have given their consent.

3. Separate data processing agreement no longer necessary

The new contract modules for data transfer to processors include requirements for commissioned data processing pursuant to Art. 28 para. 3 GDPR. If a company concludes the new SCCs, then no further data processing agreement will be required. However, an individual agreement on commissioned data processing is more difficult now because the rigid SCCs would have to be modified to such end. Furthermore, doing so will only be permissible when additional clauses do not contradict the SCCs.

IV. Implementation deadlines

The new SCCs will enter into force upon their publication in the Official Journal of the EU in the upcoming weeks.

However, the former SCCs rooted in Decision 2010/87/EU will not become obsolete immediately. They may continue to be used for a transition period of three months after the new SCCs comes into force.

The following applies to former SCCs already in use: Once the three-month transition period has passed, the former SCCs will remain valid for a further 15 months for data transfer contracts already concluded. This is conditional upon the processing operations which are the subject of the data transfer contract remaining unchanged, and on additional measures being undertaken to ensure the requirements under Art. 46 para. 1 GDPR are met. Thus, the former SCCs will only retain validity in existing data transfer contracts when it is ensured that the Schrems II ruling and its requirements are being met to a sufficient degree. This can be done by, to cite one example, agreeing additional measures.

V. Outlook and recommended action for companies

It is a welcome development that the new SCCs lay down an updated and adequate foundation for data transfers to third countries. Yet conclusion of the SCCs alone will not suffice to attain legal certainty. The level of data protection in the third country must be examined actively on a case-by-case basis.

Acute action is required for companies which do carry out third-country data transfers. In particular, the following measures should be initiated or implemented:

(1) **Contracts:** For new contracts, the new SCCs must be accounted for after the three-month transition period. For old contracts, the former SCCs must be replaced with the new SCCs by no later than December 2022.

(2) **Appraisal of the situation:** As a precautionary measure, it must be (re-)verified whether and to what extent third-country service providers are used and a corresponding data transfer takes place (these service providers must, in turn, likewise verify whether they work with sub-contractors in third countries relevant for the contract).

(3) **Review of security measures:** As a precautionary measure, the technical and organisational security measures for data protection need to be reviewed (anew), including the legal protection of data in a third country.

(4) **Audit of data protection level:** The information provided on security measures must be used to audit whether an adequate level of data protection is being provided and/or can be guaranteed.

(5) **Audit records:** In the interest of being able to provide evidence, records of the data protection audit should be made.

(6) **Data protection impact assessment:** Since this will be obligatory for the new SCCs anyway, an impact assessment should be considered for existing contracts with the former SCCs; especially when the level of data protection is going to have to be reviewed (again) anyway.

German data protection authorities have begun - independently of the new SCCs - to proactively monitor whether the third-country data transfer requirements in the CJEU's Schrems II ruling are being met[1]. Therefore, companies which carry out data transfers involving third countries should take action swiftly. Since reviews will have to be performed anyway, it is recommendable to not wait until the transition period has passed, but rather to replace the former SCCs as soon as possible.

Dr. Jörg Kahler
Attorney-at-Law (Germany), partner
Berlin office
Tel +49 30 20390-70
joerg.kahler@gsk.de

Dr. Martin Hossenfelder
Lawyer, Counsel
Berlin office
martin.hossenfelder@gsk.de

Simonié Schlombs
Attorney-at-Law (Germany)
Berlin office
Tel +49 30 20390-70
simonie.schlombs@gsk.de

[1] For example, see the announcement by Berlin's data protection authority https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210601-PM-Schrems_II_Pruefung.pdf

GSK
STOCKMANN

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason we recommend you to request personal advice.

www.gsk.de

GSK Stockmann

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907-0
F +49 30 203907-44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566-0
F +49 6221 4566-44
heidelberg@gsk.de

FRANKFURT / M.
Taunusanlage 21
60325 Frankfurt am Main
T +49 69 710003-0
F +49 69 710003-144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174-0
F +49 89 288174-44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L-1855 Luxembourg
T +352 271802-00
F +352 271802-11
luxembourg@gsk-lux.com