NEWSLETTER

The new Standard Contractual Clauses

On 4 June 2021, the European Commission issued new Standard Contractual Clauses ("SCC" or "Clauses"). The new SCC entered into force on 28 June 2021[1] and shall provide an adequate level of data protection within the meaning of Article 46 (2) (c) of the General Data Protection Regulation ("GDPR"), by taking the latest CJEU's Schrems II judgment[2] into account.

Relevant dates

- The new SCC will replace the existing standard contractual clauses, and **ought to be used with effect from 28 June 2021**.
- **New data transfers must be based on the new Clauses as of 27 September 2021.**
- Contracts entered into before 27 September 2021 on the basis of the previous sets are deemed to provide appropriate safeguards for international data transfers **until 27 December 2022**, provided "*the processing operations [...] remain unchanged*".
- **As of 28 December 2022, only the new SCC may be used.**

Material scope

- The main focus of the Clauses is the protection of personal data transferred between a party located inside and a party located outside the EEA.
- However, the Clauses are also applicable to data transfers between non-EEA parties, if one of the parties is subject to the GDPR for offering goods or services to EU customers (Article 3(2) GDPR).[3]
- More than two parties can enter into, and further parties may accede to, the Clauses by using the so-called Docking Clause (Clause 7).

1 The 20th day after the publication of the SCC in the Official Journal of the European Union (7 June 2021 L 199/31).

2 CJEU, judgment dated 16 July 2020 (C-311/18).

3 Now clarified in Recital 7 and Clause 13 (a).

– "*To cater for various transfer scenarios and the complexity of modern processing chains*" (Recital 10), the SCC pursue a modular approach. The Clauses are designed as one single contract based on a modular set for four different types of data transfers, namely:

  (1) The transfer of personal data from GDPR-controller(s)[4] to Non-GDPR-controller(s)[5] (**module 1**).

  (2) The transfer of personal data from GDPR-controller(s) to Non-GDPR-processor(s) (**module 2**).

  (3) The transfer of personal data from GDPR-processor(s) to Non-GDPR-sub-processor(s) (**new module 3**).

  (4) The transfer of personal data from GDPR-processor(s) to Non-GDPR-controller(s) (**new module 4**).

Important (new) provisions

Liability

The Clauses' liability regime varies from module to module.
However, the following general liability principles apply:

– Each party is liable to the other party for any damages caused by its breach of the Clauses.

– Regardless of the existence of a contract between a party and the data subject, each party is liable to the data subject when "*breaching the third-party beneficiary rights*", which are incorporated in the SCC for all modules.

– Joint and several liability applies when more than one party is responsible for the damage caused to the data subject.

– Liability extends to non-material damages.

– Each party is liable for its processors or its sub-processors.

Data transfer impact assessment

Taking into account the Recommendations 01/2020 of the European Data Protection Board regarding the impact of the CJEU's Schrems II judgment[6], the Clauses contain detailed provisions on the so-called data transfer impact assessment.

– Both parties warrant that they have no reason to believe that the law and practices in the third country prevent the data importer from fulfilling its obligations under the Clauses.

– Both parties must also conduct a proper assessment taking into account the specific circumstances of the transfer, such as the type of recipients; intended onward transfers; the purpose of processing; the categories and format of the transferred personal data;

4 Entities which are located in the EEA or which are subject to the GDPR according to Article 3(2) GDPR.

5 Entities which are neither located in the EEA nor are subject to Article 3(2) GDPR.

6 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, see https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

the economic sector in which the transfer occurs; the storage location of the data transferred as well as the laws and practices of the third country; and the relevant contractual, technical and organisational measures.

– When carrying out the assessment, which must be documented and provided to the competent supervisory authority upon request, the data importer must cooperate with the data exporter, provide the data exporter with relevant information and notify the data exporter if new law prevents compliance with the SCC.
– The data exporter shall suspend the data transfer if no appropriate safeguards for the transfer can be put in place.

Data access (requests) by public authorities

Under the SCC, the data importer has detailed obligations concerning the handling of data access (requests) by public authorities. These include:

– After receiving an access request, or becoming aware of any direct access by a public authority, the data importer shall notify the data exporter (and where possible the data subject) of the request, providing all available information and shall, if possible, update the data exporter on the relevant request(s).
– Where the laws of the data importer's destination prohibit the abovementioned notification, the data importer must employ its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible.
– The data importer must review the legality of a governmental request for disclosure and challenge it in case of suspected unlawfulness.
– When responding to a request for disclosure, the data importer must fulfil documentation obligations and apply the principle of data minimisation.

Transparency and data subjects' rights

The Clauses strengthen the data subjects' rights, such as the right to transparent information; right of access; right to rectification, restriction, objection, etc., and impose corresponding transparency obligations on the data importer and data exporter.

Processors and sub-processors

The new SCC simplify the engagement of processors and sub-processors:

– No additional data processing agreement(s) under Article 28 GDPR are required if a controller and a processor enter into the SCC.
– A data importer outside the EEA who intends to engage a sub-processor in the third country still requires prior authorisation from the data exporter, which can now be a specific authorisation or a general authorisation for the engagement of a sub-processor from an agreed list, with a right to object within an agreed notification period.

Supplementary measures

– According to the CJEU, data exporters are responsible for verifying, on a case-by-case basis, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards, and therefore, if "*supplementary measures*" need to be adopted to ensure an adequate level of protection. The same applies to the new Clauses.[7]

– The choice of adequate supplementary measures requires an evaluation of the risks related to the data transfer, in particular concerning data access (requests) by public authorities. Once the data exporter has assessed the data transfer impact, the parties may use the technical and organisational measures described in Annex II of the SCC as a "*practical toolbox to comply with the Schrems II judgment*".[8]

Next steps

We recommend the following next steps:

Existing data transfers

(1) Identify and map existing data transfers. This exercise requires a joint effort from different departments of your company, as well as appropriate allocation of time and resources.

(2) Identify the tool which secures the data transfer. For data transfers to the UK, controllers may rely on the recent adequacy decision issued by the Commission on 28 June 2021.[9]

(3) Determine whether supplementary measures are necessary to secure the data transfer by conducting a risk-based and case-by-case data transfer impact assessment, taking into account the elements set forth in Clause 14.

(4) If the data transfer has been secured by the former standard contractual clauses, talk to your data importer about signing the new Clauses and implementing supplementary measures if and where necessary.

New data transfers should be assessed and secured with the new Clauses as well as, where necessary, supplementary measures.

If you require assistance with this undoubtedly tremendous task, we would be happy to assist you.

7 This is clarified in the Clauses themselves (Clause 14 (b) (iii)) and highlighted, e.g., in the press statement of the German Conference of the Independent Data Protection Authorities of the Federation and the States („Datenschutzkonferenz"), press release of the DSK, dated 21 June 2021, see: www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf.

8 See press release of the European Commission, dated 4 June 2021 „European Commission adopts new tools for safe exchanges of personal data", see https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

9 Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (C(2021) 4800 final), see https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

Contact

Vera Jungkind
Partner
T +49 211 8304 405
vera.jungkind@hengeler.com

Alla Drößler
Director Compliance
Senior Associate
T +49 211 8304 764
alla.droessler@hengeler.com

Wolfgang Spoerr
Partner
T +49 30 20374 161
wolfgang.spoerr@hengeler.com

Dirk Uwer
Partner
T +49 211 8304 141
dirk.uwer@hengeler.com

Susanne Koch
Counsel
T +49 211 8304 132
susanne.koch@hengeler.com

Anna Eickmeier
Senior Associate
T +49 30 20374 314
anna.eickmeier@hengeler.com

Thomas Ruthemeyer
Senior Associate
T +49 211 8304 715
thomas.ruthemeyer@hengeler.com

Michael Schramm
Senior Associate
T +49 30 20374 723
michael.schramm@hengeler.com

www.hengeler.com

LINKS

- EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021 (PDF)
- Press statement of the German Conference of the Independent Data Protection Authorities of the Federation and the States („Datenschutzkonferenz"), press release of the DSK, dated 21 June 2021 (PDF)
- Press release of the European Commission, dated 4 June 2021 „European Commission adopts new tools for safe exchanges of personal data" (PDF)
- Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (C(2021) 4800 final) (PDF)