GIBSON DUNN

European Commission Adopts New Standard Contractual Clauses for International Data Transfers and Data Processing Agreements

Client Alert | June 14, 2021

On 4 June 2021, the European Commission adopted two implementing decisions containing standard contractual clauses for the processing and transfer of personal data in compliance with the General Data Protection Regulation ("GDPR").[1] In particular, these decisions adopt:

- standard contractual clauses ("New SCCs") for controllers and processors to provide appropriate safeguards regarding personal data transfers out of the European Economic Area ("EEA") to third countries not recognised by the European Commission as ensuring an adequate level of protection for personal data (and which replace the standard contractual clauses adopted in 2001 and 2010 under the Data Protection Directive 95/46/EC, the "Old SCCs");[2] and
- standard contractual clauses for the protection of personal data in the context of data processing agreements under Article 28 of the GDPR ("DPAs") between controllers and processors (including within the European Economic Area, or "EEA").[3]

These decisions aim to provide more complete contractual instruments for companies to execute prior to processing or transferring personal data from within the EEA, in line with the new requirements contained in the GDPR. Unlike the Old SCCs, which only applied to controller-to-controller ("C2C") and controller-to-processor ("C2P") transfers outside of the EEA, the New SCCs include different modules that parties may select and complete depending on the circumstances of the transfer (C2C, C2P, P2P, and P2C). Furthermore, the New SCCs applicable to transfers of personal data outside the EEA take into account the ruling of the Court of Justice of the EU ("CJEU") of 16 July 2020 in the *Schrems II* judgment.

The New SCCs are of particular interest for European or U.S. companies and organisations, in particular those who could not rely on the Old SCCs to transfer data outside the EEA (because transfers did not occur in the C2C or C2P context addressed by the Old SCCs), or those companies and organisations whose transfers of personal data were compromised since the annulment of the EU-U.S. Privacy Shield.

Although the new standard contractual clauses can be used as of 27 June 2021, the European Commission has put in place two grace periods for the New SCCs applicable to transfers of personal data outside of the EEA. The first grace period allows controllers and processors to execute the Old SCCs until 27 September 2021. The second grace period allows controllers and processors to rely on Old SCCs executed before 27 September 2021, until 27 December 2022. As of the latter date, companies that relied on Old SCCs to transfer personal data outside of the EEA are expected to have fully transitioned to the

Related People

Ahmed Baladi

Ryan T. Bergsieker

Kai Gesing

Vera Lukic

Clémence Pugnet

New SCCs.

This Client Alert aims to help explain the potential uses of these new standard contractual clauses.

I. Context

Under the GDPR, the European Commission has the power to adopt implementing acts, in particular: (i) creating standard contractual clauses for DPAs between controllers and processors and between processors and sub-processors (Article 28(7) of the GDPR), and (ii) creating standard contractual clauses as an appropriate safeguard for transfers of personal data to third countries (Article 46(2)(a) of the GDPR).

The implications of the adoption of these standard contractual clauses by the European Commission are different for both scenarios.

On one side, the standard contractual clauses for DPAs aim to provide an optional set of clauses that controllers and processors may use to execute contracts in compliance with Article 28 of the GDPR. However, any DPA is directly subject to Article 28 of the GDPR, and does not require the use of clauses approved by the European Commission or by EU supervisory authorities to be valid. Furthermore, numerous supervisory authorities have published and issued similar sample or template DPAs to give guidance to controllers and processors.[4] However, the standard contractual clauses for DPAs adopted by the European Commission may give additional comfort to companies and organisations that engage in cross-border processing of personal data and could not rely on any guidance offered by their (lead) supervisory authority.

On the other hand, like the Old SCCs adopted under Directive 95/46/EC, the New SCCs adopted for transfers of personal data outside of the EEA have a greater importance for companies and organisations. They may be considered to be *de facto* binding in most circumstances, as they are the most accessible and affordable framework from those available under the GDPR to transfer personal data to third countries. The execution and application of New SCCs allows entities to transfer personal data to third countries without the direct and immediate intervention of or notification to any EU supervisory authority.[5]

Since last year, the adoption of the New SCCs had become a pressing political and legal issue at the EU level. On 16 July 2020, the CJEU adopted the *Schrems II* judgment, which invalidated the EU-U.S. Privacy Shield. Numerous companies had relied on this framework to transfer personal data from the EEA to the U.S. and to provide assurances that this data would be protected after the transfer. The CJEU's ruling confirmed the validity of the Old SCCs adopted under Directive 95/46/EC (before the GDPR), but required companies to verify, prior to any transfer of personal data pursuant to the SCCs, whether data subjects would be granted a level of protection in the receiving country essentially equivalent to that guaranteed within the EU. These requirements have been addressed and explained by the European Data Protection Board ("EDPB") in two recommendations issued on 10 November 2020, and were discussed in a previous client alert.

Against this backdrop, the European Commission initiated the process for the adoption of these standard contractual clauses on 12 November 2020, when it adopted draft implementing decisions for the New SCCs and for standard contractual clauses for DPAs. The decisions adopted on 4 June 2021 take into account the joint opinion of the EDPB and the European Data Protection Supervisor ("EDPS"), the feedback of stakeholders, and the opinion of Member States' representatives.

II. The implementation of the New SCCs under Articles 46(1) and (2)(c) of the GDPR

The New SCCs adopted by the European Commission for transfers of personal data outside of the EEA put in place a different and more comprehensive approach to data transfers than the Old SCCs adopted under Directive 95/46/EC in 2001 and 2010.

The Old SCCs were specific contractual instruments adopted by the European Commission to address specific situations: C2C transfers (the 2001 SCCs) and C2P transfers (the 2010 SCCs).

Under the New SCCs, the European Commission has adopted a single set of clauses within a contract, composed of three kinds of provisions: (i) fixed clauses, which are intended to remain unmodified regardless of the parties that execute the New SCCs; (ii) modules, which are intended to be added/removed from the final contract depending on the parties that execute the New SCCs (C2C, C2P, P2C, and P2P) and their choice among the options available; and (iii) blank clauses and annexes, which are to be filled in and completed by the parties with relevant information (*e.g.*, the categories of data transferred, the data subjects concerned, *etc*.).

As can be seen, the New SCCs are intended to be live and adaptive instruments that can be tailored as needed. First, this modular approach allows the parties to address various transfer scenarios and the complexity of modern processing chains. Second, the New SCCs enable the possibility of adding more than two parties to the contractual arrangement, both at its execution and during its lifetime.

It should be noted that, where the data importer is a processor or a sub-processor, the New SCCs include the DPA requirements of Article 28(2) to (4) of the GDPR. This should make the execution of two instruments (DPAs and the New SCCs) unnecessary in data transfer scenarios, as the use of the New SCCs alone would cover both requirements under Article 28 and Article 46 of the GDPR. Where two or more parties execute a DPA and the New SCCs to govern a controller-processor relationship, the terms of the latter will prevail over those of the former or over any other instrument governing the data processing terms applicable to the parties.

From a substantive perspective, the New SCCs bring along a series of novelties compared to the Old SCCs adopted under Directive 95/46/EC. The New SCCs reinforce data subjects' rights, by entitling them to be informed about data processing operations, to have a means to contact foreign controllers, to receive a copy of the New SCCs, and to be compensated for damages occurred in relation to their personal data.

In order to ensure the effective application and enforcement of the New SCCs against data importers established in third countries, the New SCCs provide that data importers shall submit to the jurisdiction of relevant EU supervisory authorities and courts, and shall commit to abide by any decision under the applicable Member State law. Also, by entering into the New SCCs, data importers agree to respond to enquiries, submit to audits (including inspections at its premises or physical facilities), and comply with the measures

adopted by the relevant supervisory authority.

In light of the abovementioned *Schrems II* ruling of the CJEU, the European Commission has supplemented the New SCCs with a number of specific measures that aim to address any effects of the laws of the third country on the data importer's ability to comply with the New SCCs. In particular, data exporters and importers that execute the New SCCs will warrant that "they have no reason to believe" that the laws and practices in the third country of destination prevent the data importer from fulfilling its obligations under the New SCCs. This representation is intended to be based on an assessment that needs to be documented, and whose disclosure may be requested by EU supervisory authorities.[6]

Furthermore, data importers entering into the New SCCs commit to the following main obligations:[7]

- To notify the data exporter if it has reason to believe that it is not able to meet the New SCCs' requirements and, in such case, add complementary measures to address the situation, or, if not possible, suspend the transfer.
- To notify the data exporter and the data subject when receiving legally binding requests from public authorities, or if not possible, provide the data exporter with as much relevant information as possible and aggregated information at regular intervals.
- To challenge the legally binding request if it has reasonable grounds to consider that request unlawful.

III. The implementation of the new standard contractual clauses for DPAs under Article 28(7) of the GDPR

The GDPR mandates that, when a controller engages a processor to process personal data on its behalf, this relationship shall be governed by a contract or other written legal act, that is binding on the processor *vis-a-vis* the controller, and that contains the elements listed in Articles 28(2) to (4) of the GDPR. These requirements are further explained in the EDPB Guidelines 07/2020, that are still under public consultation.[8]

The standard contractual clauses for DPAs adopted by the European Commission on 4 June 2021 therefore aim to provide a single and *prima facie* lawful DPA that companies and organisations can rely upon and execute to govern their controller-processor relationship.

As indicated above, since the GDPR was adopted, a number of EU supervisory authorities had issued their own DPA drafts and templates in order to provide an easy-to-implement tool for entities to comply with the GDPR. Although the European Commission's standard contractual clauses arrive some years after these national DPA templates have been adopted, they are expected to enhance the consistent application of the GDPR within the

EU.

The standard contractual clauses for DPAs contain all elements referred to by Article 28 of the GDPR for controller-processor agreements to be valid. In some sections, they allow parties some margin of maneuver, for example, by providing two options for the use of sub-processors (*i.e.*, prior specific authorisation or general written authorisation). Also, the implementing decision of the European Commission specifies that the standard contractual clauses laid can be used in whole or in part by the parties as part of their own DPAs, or within a broader contract.

The use of these standard contractual clauses for DPAs will give to controllers and processors a level of additional certainty regarding their compliance with Article 28 of the GDPR, in particular *vis-à-vis* supervisory authorities or before national courts in case of litigation. Although DPAs that do not follow the standard contractual clauses of the European Commission or of supervisory authorities are not *per se* illegal, they are expected to be subject to detailed scrutiny if they are subject to dispute or if they come under the authorities' cross-hairs.

IV. The timeline

The decisions on the standard clauses for DPAs and the New SCCs were adopted by the European Commission on 4 June and published in the EU's Official Journal on 7 June 2021. They will enter into force 20 days after their publication, *i.e.*, on 27 June 2021.

The decision relating to the New SCCs for transfers of personal data to third countries provide for two transitional (or grace) periods in order to allow stakeholders to change their contractual frameworks.

- *First*, the Old SCCs adopted under Directive 95/47/EC will be valid for an additional period of three months, until 27 September 2021, when they will be repealed. This means that, until 27 September 2021, companies and organisations can continue executing the Old SCCs to cover their data transfers outside the EEA. After this date, entities are meant to only execute the New SCCs.
- *Second*, the Old SCCs executed before 27 September 2021 will be considered to be valid for an additional period of 15 months, until 27 December 2022. After this date, companies are expected to have transitioned the Old SCCs governing their data transfers outside the EEA to the New SCCs.

V. Consequences

The publication of the final version the standard contractual clauses and, especially, the New SCCs on personal data transfers to third countries, were widely anticipated.

The update and upgrade brought about by the New SCCs was considered by many to be necessary, given the importance attached by numerous EU supervisory authorities to ensuring the protection of personal data transferred outside the EEA. The New SCCs are subject to the strictures of being fixed (*i.e.*, any changes would need to be authorised by the competent EU supervisory authority) and requiring significant substantial obligations on the data importer. Notwithstanding this, they remain a preferred cost-effective option to govern data transfers outside of the EEA, as other options for entities to continue transferring personal data are generally more burdensome or costly.

EU companies, in particular those dealing with U.S. companies and that have been in a stand-by situation since the *Schrems II* ruling in July 2020, are advised to consider initiating agreement renewals using the New SCCs. Companies in the U.S. and in other countries not recognised by the EU as granting an adequate level of protection are also recommended to review and become acquainted with the New SCCs, as they may need to implement in their offerings the new terms and the many new obligations that data importers will have to comply with by 27 September 2021. By 27 December 2022, all agreements executed under the Old SCCs will need to have been transitioned to the New SCCs.

---

[1] *See* Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council; *and* Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[2] *See* Article 46(1) and (2)(c) of the GDPR.

[3] *See* Artic le 28(7) of the GDPR.

[4] *See* Article 28(8) of the GDPR, which also enabled EU supervisory authorities to adopt standard contractual clauses for DPAs. See, for example, the French *CNIL* (https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses); the Spanish *AEPD* (https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf). Denmark, Slovenia and Lithuania have also submitted to the European Data Protection Board ("EDPB") draft standard contractual clauses for DPAs under Article 28 of the GDPR.

[5] Unlike other frameworks for the transfer of personal data outside the EEA, foreseen by Articles 46 and 47 of the GDPR, such as Binding Corporate Rules ("BCRs"), approved codes of conduct and certification mechanisms, or even *ad hoc* contractual clauses negotiated privately among controllers and/or processors. All these mechanisms require or assume the intervention of a supervisory authority or a certified/approved third party to supervise and authorise the transfer of personal data outside of the EEA.

[6] *See* New SCCs, Clause 14.

[7] *See* New SCCs, Clause 15.

[8] *See* Guidelines 07/2020 on the concepts of controller and processor in the GDPR, *available at*: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en.

The following Gibson Dunn lawyers prepared this client alert: Ahmed Baladi, Ryan T. Bergsieker, Kai Gesing, Alejandro Guerrero, Vera Lukic, Adelaide Cassanet, and Clemence Pugnet.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please also feel free to contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Data Innovation practice group:

Europe
Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)

James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

United States
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation