ALERT MEMORANDUM

New Standard Contractual Clauses for Data Transfers under the GDPR – New Changes, New Questions?

July 6, 2021

On June 4, 2021, the European Commission (the "**Commission**") published its new standard contractual clauses for transferring personal data from the EU to third countries pursuant to the General Data Protection Regulation 2016/679 (the "**New SCCs**"). The previous set of standard contractual clauses (the "**Old SCCs**") will be repealed with effect from September 27, 2021, and any contracts implementing the Old SCCs will no longer be deemed to provide appropriate safeguards under the GDPR from December 27, 2022, forcing organisations to revise their existing contractual structures. The New SCCs are also intended to address the requirements arising from last year's CJEU judgment in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("***Schrems II***") and align with guidance from the EDPB[1].

Overall, the New SCCs are welcomed for addressing many of the issues that organisations have been facing when using the original sets of clauses (such as how to address processor-to-processor transfers).[2] However, a number of questions remain and new questions have arisen. The New SCCs also have to be read in combination with the final EDPB *Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (the "**EDPB Recommendations**"),[3] which provide examples of acceptable supplementary measures.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

LONDON

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

Louie Ka Chun
+44 20 7614 2361
klouie@cgsh.com

2 London Wall Place
London EC2Y 5AU
T: +44 20 7614 2200

BRUSSELS

Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2000

ROME

Federica Mammì Borruto
+39 06 6952 2826
fmammiborruto@cgsh.com

Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21

[1] EDPB, Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, June 18, 2021.

[2] Such transfers are now covered by Module 3 of the New SCCs.

[3] EDPB, Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, June 18, 2021.

I. Evolution of Standard Contractual Clauses from Directive to GDPR

The previous set of standard contractual clauses were adopted by the Commission in 2001 (as amended in 2004) and in 2010, under the precursor to the GDPR, the Data Protection Directive (Directive 95/46/EC). They consisted of two models of standard contractual clauses, addressing data transfers from EU-based data controllers to non-EU-based data controllers[4] and another set addressing data transfers from EU-based data controllers to non-EU-based data processors.[5] The Old SCCs were adopted by the Commission pursuant to Article 26(4) of the Data Protection Directive, providing data exporters with a mechanism under which to transfer data to third countries.

After the CJEU's ruling in *Maximillian Schrems v. Data Protection Commissioner* ("***Schrems I***") which invalidated the adequacy decision underpinning the old Safe Harbour (for more details on the *Schrems I* judgment, please see our previous alert memorandum here), many organisations moved to SCCs for their international data transfers. The increasing complexity of cross-border data processing and transfers made some of the challenges of the Old SCCs evident and apart from the necessary adaptation of such clauses to the novel aspects of the GDPR, the need for an update was further accelerated when the CJEU handed down the *Schrems II* judgment (for more details on the *Schrems II* judgment, please see our previous post here). Although the court upheld the Old SCCs, organisations were now required carefully to assess whether the laws of the recipient country comply with the material terms of the Old SCCs and afford the same level of protection as provided under the GDPR, failing which additional safeguards must be put in place.

On November 12, 2020, the Commission published its draft for the modernised form of standard contractual clauses that would (with some changes) ultimately become the New SCCs, and opened a consultation on the draft on the same day. By closing of the consultation on December 10, 2020, the Commission had received feedback from 148 respondents, the majority being business associations and company/business organisations.[6]

On June 4, 2021, the Commission published its Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries (the "**Implementing Decision**"), which sets out the New SCCs.[7]

The Implementing Decision repeals the previous Commission decisions implementing the Old SCCs, with effect from September 27, 2021. In addition, the Implementing Decision provides for a grace period – any contracts implementing the Old SCCs concluded before September 27, 2021 will be deemed to provide appropriate safeguards (subject to the *Schrems II* judgment) until December 27, 2022.[8] This creates an overlap period of approximately three months whereby a data exporter can choose between the Old SCCs and New SCCs for any new data transfers. However, any agreements incorporating the Old SCCs will have to be updated before December 27, 2022 regardless.

II. Main differences between the Old SCCs and the New SCCs

The New SCCs adopt a fresh and more nimble structure in an effort to reflect the complexity of international data transfers.

Modular approach

The New SCCs combine certain general clauses with a modular approach to provide for a range of transfer scenarios. The following transfers to third countries are covered:

- Module 1: Transfer from controller to controller ("**C2C**");

[4] Decision 2001/497/EC and Decision 2004/915/EC.

[5] Decision 2010/87/EU.

[6] See, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-/feedback_en?p_id=14543795

[7] See, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[8] Article 4(4) of the Implementing Decision.

- Module 2: Transfer from controller to processor ("**C2P**");
- Module 3: Transfer from processor to processor ("**P2P**");
- Module 4: Transfer from processor to controller ("**P2C**").

This allows for a flexible combination of the applicable modules and adds the P2P and P2C modules that were previously not foreseen under the Old SCCs (which often created legal uncertainty for organisations' internal and external data flows).

C2P and P2P modules now also explicitly address the requirements under Article 28 of the GDPR for data processing agreements. In this regard, Recital 9 of the Implementing Decision clarifies that where the processing involves data transfers from controllers subject to the GDPR to processors outside its territorial scope or from processors subject to the GDPR to sub-processors outside its territorial scope, the New SCCs would also be able to fulfil the requirements of Article 28(3) and (4) of the GDPR. Accordingly, companies using the New SCCs to legitimise transfers of personal data from either a controller to a processor, or a processor to a sub-processor, are no longer required to enter into separate data processing agreements.

The "docking-clause"

While the Old SCCs were bipartite agreements – without a means for additional parties to join directly – the New SCCs contain a docking clause that would allow additional data exporters or importers to accede to the New SCCs throughout the lifecycle of the contract.

Under Clause 7 of the New SCCs, the new party may, "*by agreement of the Parties*", accede to the New SCCs at any time, either as a data exporter or as a data importer, by completing a new data transfer Appendix and signing Annex I.A.

The acceding party will have the rights and obligations arising under the New SCCs from the point of their joining (but not prior to that point).

The docking clause is a welcome way of addressing the challenges within large-scale intra-group or extra-group data transfers.

Extended geographical reach

Under the Old SCCs, the data exporter had to be established in the EU, making the tool unavailable for a data exporter established outside of the EU but still (for instance) subject to the GDPR by virtue of Article 3(2) GDPR.

By contrast, the New SCCs contain no express limitation as to the location of the data exporter. Specifically, Article 1 of the Implementing Decision states that: "*The standard contractual clauses* […] *provide* […] *appropriate safeguards* […] *for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-) processor whose processing of the data is not subject to that Regulation (data importer).*"

Consequently, the New SCCs can generally be used by a data exporter subject to GDPR, regardless of location.[9]

***The Schrems II* effect**

As anticipated, the New SCCs take account of the *Schrems II* judgment in Section III. In particular, the New SCCs set forth:

- an obligation on the data exporter (assisted by the data importer) to consider the level of protection of personal data in the country outside the EEA;
- an obligation on the data importer to notify the data exporter of any inability to comply with the New SCCs, and a related obligation on the exporter to suspend data transfers or terminate the agreement.

[9] And with the exclusions provided in Recital 7, namely where the processing by the importer already falls within the scope of the GDPR. See further below, III. Certain questions remain.

In this context, the parties have to warrant that, at the time of signing the New SCCs, they have *no reason to believe* that the laws and practices applicable to the data importer, including any requirements around disclosure to, or access by, public authorities, prevent the data importer from complying with the New SCCs.

Transfer impact assessments

The parties must carry out a "*transfer impact assessment*", which must also be made available to the competent supervisory authority, upon request.

Data exporter and data importer must:

- consider the specific circumstances of the transfer, such as the content and duration of the contract, the nature of personal data to be transferred, the length of processing chain, the type of recipient, the transmission channels used, and purposes of the processing;
- assess that laws and practices in the third country of destination respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR;
- put in place any relevant contractual, technical or organisational safeguards to supplement those under the SCCs, and ensure a level of protection essentially equivalent to that guaranteed within the EU, including with regard to security and confidentiality.

The assessment of laws and practices should include reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. However, if the parties wish to rely on their practical experience of public authority access to data, it "*needs to be supported by other relevant, objective elements*" (see footnote 12 of the New SCCs). Specifically, the parties have to take into account whether their experience is corroborated and not contradicted by publicly accessible and reliable information on public authority requests to access personal data within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

While this is not to be understood as a departure from the stringent documentation requirement of a fact-based analysis, the wording of clause 14 of the new SCCs in combination with footnote 12 appears to be closer to the generally risk-based approach of the GDPR, allowing for certain experience-based elements to be part of the assessment. A more risk-based approach would be welcomed, ensuring that the burden on organisations in complying with their data protection obligations is not insurmountable.

Companies transferring personal data to U.S. might in the future be able to take into account publications such as the White Paper introduced by the Department of Commerce, in September 2020[10], which was intended to provide transparency with respect to information relevant to the transfer impact assessment after *Schrems II*. The White Paper stipulates that most U.S. companies do not transfer data of interest to U.S. intelligence agencies, which results in a low risk profile. The paper also provides further insight into FISA 702 and EO 12333 and points to other public resources that would be of assistant for an assessment.

It is to be expected that over time a body of potentially sector-specific assessments of the risks in various jurisdictions can be developed in a more standardised manner, which can then hopefully form (approved) building blocks of the necessary documentation.

[10] See https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

EDPB Recommendations

The EDPB Recommendations are now also overall aligned with this approach.[11] Departing somewhat from its prior position in the draft Recommendations,[12] the EDPB has included more language that suggests acceptance of the parties taking into account *practices* of the third country insofar as they have an impact on the effective application of the safeguards contained in the Article 46 GDPR transfer tool.[13] However, the EDPB also stressed that the absence of prior instances of requests for access received from public authorities are not a decisive factor.[14] The required assessment has to be conducted with due diligence and documented in a detailed report.[15]

New Data Importer Obligations

For the SCCs, Section III now imposes obligations on a data importer in case of a binding request for disclosure from a public (including judicial) authority: there is an obligation on the data importer to: (i) notify both the data exporter and data subjects of the request (where possible), providing the data exporter with "*aggregate information at regular intervals*" (see Recital 22 of the Implementing Decision and Clause 15.1); (ii) document the request, the steps it followed, and its response (which must be made available to the data exporter and/or the competent supervisory authority, upon request; see Clause 15.2(b)); and (iii) challenge the request where the data importer concludes there are reasonable grounds to consider it unlawful by reference to the laws of the third country and its international commitments, including by "*exhausting available possibilities of appeal*" (see Recital 22 of the Implementing Decision and Clause 15.2(a)).[16]

III. Certain questions remain

Interaction of Art. 3(2) and Chapter V of the GDPR?

Recital 7 of the Implementing Decision notes that the New SCCs are for use "*without prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679. The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679*" – this would include the transfer of personal data by a controller or processor not established in the EU, to the extent that the processing is subject to the GDPR (pursuant to Article 3(2) thereof). The question that arises is whether moving data to an importer subject to Art. 3(2) GDPR constitutes a transfer in the sense of Chapter V of the GDPR. The Commission has left this definition to the EDPB or eventually the Court by including the "*without prejudice*" wording in Recital 7. Further guidance is therefore required also with respect to the appropriate transfer tool to use for such a scenario given that the New SCCs can only be used where the data importer is not subject to the GDPR.[17]

[11] For more details on the draft EDPB Recommendations issued by the EDPB on November 11, 2020, please see our previous post here.

[12] For instance the draft EDPB Recommendations did not include practices as "[e]*lements demonstrating that a third country authority will be able to access the data through the data importer or through direct interception of the communication channel*" mentioning only "*reported precedents, legal powers, and technical, financial, and human resources at its disposal*" (see § 43).

[13] The EDPB clarified that the parties could take into account reports based on practical experience with prior instances of requests for disclosure from public authorities, or from entities active in the same sector as the importer (see § 144 of Annex 3 of the EDPB Recommendations).

[14] According to the EDPB Recommendations, demonstrating that problematic legislation is not applied in practice to transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data, does not exempt the data importer and exporter from providing for the necessary supplementary measures to protect personal data during its transmission and processing in the third country of destination (e.g. end-to-end encryption of data) if the analysis of the applicable legislation of the third country of destination indicates that access to data may also take place, even in the absence of the importer's intervention, at the time of the transfer.

[15] The EDPB Recommendations clarify that reports, which should be endorsed by the legal representative of the exporter, will have to include comprehensive information on the legal assessment of the legislation and practices, and of their application to the specific transfers, the internal procedure to produce the assessment (including information on actors involved in the assessment, e.g. law firms, consultants, or internal departments) and dates of the checks.

[16] Where possible the importer must seek an interim measure with a view to suspending the effects of the request until the competent judicial authority has decided on its merits and disclose the minimum amount of personal data reasonably possible in response to the order.

[17] For instance, the parties may consider entering into *ad-hoc* clauses.

What additional safeguards should be put in place by the parties to ensure a level of protection essentially equivalent to that guaranteed within the EU?

The New SCCs do not clarify which effective measures data importers and data exporters should put in place in order to ensure an essentially equivalent level of protection for personal data. They only state that the parties should consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.[18]

The parties will have to look to the EDPB Recommendations for further clarity. In this regard, the EDPB Recommendations offer a (non-exhaustive) list of factors to identify which measures would be most effective in protecting the data transferred from public authorities' requests for access, including the format of the data to be transferred (i.e., in plain text/pseudonymised or encrypted), nature of data, length and complexity of data processing workflow, number of actors involved in the processing, and the relationship between them, parameters of practical application of the third country law, and the possibility that the data may be subject to onward transfers. In addition, Annex 2 of the EDPB Recommendations provides examples of technical, contractual and organisational supplementary measures.[19]

The application of Module 4

Module 4 concerns transfers of personal data from a processor to its appointing controller. This appears to clarify at least from the Commission's point of view that a re-transfer of data from a processor subject to GDPR to a controller that is not subject to GDPR constitutes a transfer under Chapter V, regardless of the origin of the data. While Module 4 certainly has a lighter touch than the other modules in terms of obligations for the importer, invoking clause 14 only in certain circumstances still has the awkward effect of the processor imposing SCCs for the return of data that in many cases may not have been subject to GDPR at its origin. This might have a chilling effect on non-EU organisations choosing EU-based processors in the future.

Can the parties amend the liability provisions of the New SCCs?

Pursuant to Recital 3 of the Implementing Decision, the data exporter and the data importer are free to include the New SCCs in a wider contract, and "*to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly,*" the New SCCs or prejudice the fundamental rights or freedoms of data subjects.

In light of the above, would limiting liability only as between the parties "contradict" this provision, where liability towards data subjects or competent supervisory authorities remains untouched?[20] This is often a contentious negotiation point and more clarity would be useful.

IV. Divergence with SCCs under the UK GDPR

Since the end of the transition period[21] on December 31, 2020, EU law (and Commission Decisions) are no longer directly applicable in the UK. As such, the New SCCs will not apply for transfers of personal data from the UK to a third country. Under the UK GDPR, the Old SCCs continue to be effective until the UK Information

[18] In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject must, where possible, remain under the exclusive control of the data exporter.

[19] The EDPB Recommendations consider that encryption provides an effective supplementary measure. However, there are cases where unencrypted personal data is technically necessary for the provision of the service or the data importer needs to be in possession of the cryptographic keys. In these cases, according to the EDPB Recommendations, transport encryption and data-at-rest encryption, even taken together, are not considered sufficient to ensure an essentially equivalent level of protection (see Case 6 in Annex 2 of the EDPB Recommendations). In these cases, since according to the EDPB Recommendations, contractual and organisational measures alone generally are not sufficient, data controllers and processors risk being required to suspend the transfer of personal data to certain third countries in the future where the supplementary measures are considered not effective.

[20] This question is challenging given that the SCCs expressly state that "*each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses*" (see Clause 12 of the New SCCs).

[21] This transition period was in place following the UK's withdrawal on January 31, 2020 from the European Union and the European Economic Area.

Commissioner's Office ("**ICO**") publishes its own SCCs (the "**UK SCCs**"). The ICO intends to consult on and publish UK SCCs during 2021.[22]

At this time, it is unclear whether the UK SCCs would be substantially similar to the New SCCs. This could result in a divergence in approach between documents governing data transferring from the EU to a third country, and documents governing data transferring from the UK to a third country, especially impacting organisations that operate in both the EU and the UK. Organisations that export personal data both out of the EU to third countries and out of the UK to third countries should be prepared to adopt separate sets of standard contractual clauses for each of these data flows.

As mentioned above, the Old SCCs will no longer be valid from December 27, 2022 in relation to data transfers out of the EU. With uncertainty as to when the ICO would publish and adopt the UK SCCs, organisations looking to begin the process of revising their standard contractual clauses to the New SCCs may find themselves repeating the exercise for data transfers out of the UK once the UK SCCs are adopted.

Further, the Commission has, on June 28, 2021, adopted two adequacy decisions in respect of the UK,[23] prior to the expiry of the provisions on transfer of personal data within the EU-UK Trade and Cooperation Agreement[24] at the end of June. As such, personal data can continue to freely flow from the EU to the UK, and no standard contractual clauses are required.[25]

V. Conclusions

The New SCCs will require considerable effort and investment in terms of implementation into the complex structures of modern transfer chains. Organisations should:

- assess which of their data transfers are covered by SCCs, which jurisdictions are implicated, and how best to replace their Old SCCs with the appropriate New SCCs (including whether transfers would now be covered by one of the new modules);
- where SCCs form part of other contracts, assess how the New SCCs interact with the existing provisions of the contract, such as indemnities, risk allocation and limitations of liability;
- ensure a timely move to the New SCCs by December 27, 2022.[26]

The hope is that the data protection agencies will lean towards compliance rather than heavy fines until all sides have had a chance to assess and find potential avenues forward. Once organisations have implemented the New SCCs, there may also be a question as to the collective appetite for a new Privacy Shield mechanism, if one were to be negotiated again, considering the high likelihood of a renewed challenge with an uncertain outcome.

…

CLEARY GOTTLIEB

[22] See, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/

[23] See, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183. This followed the EU member states' formal approval of the draft adequacy decision on June 16, 2021 (see, here and here).

[24] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, December 31, 2020.

[25] Please note that, in light of a recent judgment of the England and Wales Court of Appeal, transfers for the purposes of UK immigration control are excluded from the scope of the adequacy decision.

[26] This includes instances where the Old SCCs are still implemented during the current grace period, because negotiations may be too far progressed.