European Commission's International Data Transfer Standard Contractual Clauses: What Businesses Need to Know

by David Dumont and Bridget Treacy, with assistance from James Henderson and Olivia Lee, Hunton Andrews Kurth LLP, with Practical Law Data Privacy Advisor

Articles | Published on 25-Aug-2021 | European Union, Switzerland, United Kingdom

An Article discussing the background to and key takeaways from the European Commission's new standard contractual clauses (SCCs) for the transfer of personal data from the European Economic Area (EEA) to countries not offering an adequate level of protection. This Article also discusses the new SCCs' status in the UK and Switzerland and next steps for businesses.

On June 4, 2021, the European Commission adopted final versions of two Implementing Decisions on standard contractual clauses (SCCs):

- Implementing Decision and Annex on SCCs for the transfer of personal data from the EEA to third countries (New Transfer SCCs).
- Implementing Decision and Annex on SCCs between controllers and processors under GDPR Article 28(7) (Article 28 SCCs).

(For more, see Legal Update, European Commission adopts final versions of standard contractual clauses under EU GDPR and Article, Key Takeaways From the European Commission's Article 28 Standard Contractual Clauses.)

Beginning September 27, 2021, the New Transfer SCCs replace existing European Commission SCCs adopted under the EU Data Protection Directive (95/46/EC) (Data Protection Directive), specifically:

- Commission Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (June 15, 2001) (2001 Clauses) for controller-to-controller transfers.
- Commission Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (December 27, 2004) (2004 Clauses) for controller-to-controller transfers and amending the 2001 Clauses.
- Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (February 5, 2010) (2010 Clauses), repealing Commission Decision 2002/16/EC on standard contractual clauses for the transfer of personal data to processors established in third countries (December 27, 2001).

The EU data protection regime has changed significantly since the European Commission's adoption of the 2001, 2004, and 2010 Clauses due to the implementation of the GDPR, the exponential growth in data flows and international data transfers, and the recent European Court of Justice (ECJ) decision that declared the EU-US Privacy Shield invalid (*Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case

C-311/18) EU:C:2020:559 (*Schrems II*); see Impact of *Schrems II* and Legal Update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ)).

SCCs are one of the most widely used mechanisms to enable international data transfers and have become the default alternative for UK and EU data transfers to the US following *Schrems II*. However, the existing SCCs were outdated and in need of revision, referring to the Data Protection Directive requirements and failing to provide a compliant data transfer solution for common data transfer scenarios, such as data transfers by processors.

The New Transfer SCCs resolve certain practical issues faced by organizations using the existing SCCs but also introduce new and more onerous obligations for data transfers outside the EEA. This Article discusses the key takeaways for the New Transfer SCCs. For more on the Article 28 SCCs, see Article, Key Takeaways from the European Commission's Article 28 Standard Contractual Clauses.

For more on the impact of the New Transfer SCCs for UK organizations, see Article, European Commission's new standard contractual clauses: what they mean for UK businesses.

GDPR Data Transfer Requirements

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the retained EU law version of the GDPR (UK GDPR) prohibit personal data transfers to a third country (Article 44, GDPR; Article 44, UK GDPR). Controllers and processors may only transfer personal data to a third country:

- Based on a determination by the European Commission that the recipient country provides an adequate level of protection (Article 45, GDPR) or adequacy regulations under the UK GDPR (Article 45(1), UK GDPR). For the European Commission's current list of countries that are deemed adequate, together with specific adequacy decisions, see European Commission: Adequacy decisions. The European Commission adopted an adequacy determination for the UK on June 28, 2021 (see Legal Update, European Commission adopts UK adequacy decisions).
- Where the controller or processor provides appropriate safeguards, if data subjects can enforce their legal rights and have effective legal remedies (Article 46, GDPR). Appropriate safeguards include standard data protection clauses adopted by the European Commission under the GDPR or the Information Commissioner's Office (ICO) under the UK GDPR (Article 46(2), GDPR; Article 46(2), UK GDPR).
- In the absence of an adequacy decision under the GDPR, adequacy regulations under the UK GDPR, or appropriate safeguards, by relying on a derogation from the data transfer prohibition (Article 49, GDPR; Article 49, UK GDPR). The derogations, which include contractual necessity and the explicit consent of the data subject, generally apply only to non-routine and occasional transfers.

For more information on cross-border data transfer mechanisms under the GDPR, see Practice Note, Overview of EU General Data Protection Regulation: Cross-border data transfers and GDPR Cross-Border Transfers Checklist.

For more on cross-border data transfers under the UK GDPR, see Data Transfers from the UK and Practice Note, Cross-border transfers of personal data (UK GDPR and DPA 2018).

Transition and Implementation

The New Transfer SCCs took effect on June 27, 2021. The 2001, 2004, and 2010 Clauses will be repealed on September 27, 2021. Organizations have until September 27, 2021, to finalize any data transfer arrangements that

have already started and that will rely on the existing SCCs. If the deadline is missed, the New Transfer SCCs must be used.

Current transfer arrangements based on the existing SCCs remain valid until December 27, 2022, if the data processing activities are unchanged and the SCCs provide appropriate safeguards. Organizations must ensure that all data transfers relying on SCCs utilize the New Transfer SCCs by December 27, 2022.

The New Transfer SCCs have not been adopted for use in the UK. These transition periods do not apply to personal data transfers from the UK (see Data Transfers from the UK).

Key Features of the New Transfer SCCs

Scope

The existing SCCs only apply to personal data transfers from an EEA-based organization to a non-EEA organization. This created data export compliance challenges for non-EEA data exporters who were subject to the GDPR under its extraterritorial scope provisions who often collect personal data directly from individuals through online platforms or websites and may transfer that personal data to other non-EEA organizations (Article 3(2), GDPR; see Practice Note, Determining the Applicability of the GDPR: Applicability for Non-EU-Established Businesses). The existing SCCs were drafted on the basis that the data exporter was EEA-based and were therefore unavailable as a lawful data transfer mechanism in this scenario.

The New Transfer SCCs resolve this issue, expressly permitting their use where the data exporter is subject to the GDPR (whether based in the EEA or not) and the data importer is not subject to the GDPR (Recital 7, GDPR). The New Transfer SCCs further support this position by deeming the supervisory authority for the jurisdiction in which the organization's EU Representative is appointed as the competent supervisory authority for the New Transfer SCCs (Clause 13, New Transfer SCCs).

The New Transfer SCCs can be used only if the data importer's processing falls outside of the GDPR's scope. If a data importer is subject to the GDPR due to its extraterritorial scope, the New Transfer SCCs cannot be used to safeguard that transfer (Recital 7). This appears to suggest that transfers to non-EEA data importers that are subject to the GDPR's exterritorial scope provisions under Article 3(2) are not subject to data transfer restrictions. While not stated explicitly, this would represent a significant change in the European Commission's approach. It is consistent with previous ICO international transfer guidance, which recognized that transfers to entities subject to GDPR Article 3(2) are not restricted transfers. If an alternative view was taken, data importers subject to the GDPR would have to execute the New Transfer SCCs, which would restate many of their preexisting direct obligations in contractual format. Further guidance from the EU and UK supervisory authorities on this topic is needed.

Modular Approach

The New Transfer SCCs adopt a new modular format covering more transfer scenarios than the existing SCCs, including modular sets of clauses for:

- Controller-to-controller transfers (Module 1).
- Controller-to-processor transfers (Module 2).
- Processor-to-processor transfers (Module 3).

- Processor-to-controller transfers (Module 4).

Organizations select the module applicable to their transfer and use the clauses specific to that module. The New Transfer SCCs introduce new SCCs for processor-to-processor and processor-to-controller transfers that were not available under the existing SCCs, providing a means of achieving legal compliance in common transfer scenarios, which was lacking under the existing SCCs. However, the new modular approach will likely create more work for organizations that previously relied on vague wording describing when each party will act as a controller or processor.

Like the existing SCCs, the New Transfer SCCs append annexes detailing the specifics of the data export arrangements. The New Transfer SCCs append:

- Annex 1, Description of the transfers.
- Annex 2, Security measures.
- Annex 3, Sub-processors.

Organizations will need to dedicate more effort to completing the annexes to the New Transfer SCCs. The New Transfer SCCs' revised format requires organizations to understand and document their data transfers in more detail and be more accountable for their data transfers, including onward transfers, than was previously the case. Organizations must complete comprehensive data mapping exercises to ensure that they have a detailed understanding of their data transfers, which should be reflected in the Annexes. Supervisory authorities are likely to apply greater scrutiny to this information following *Schrems II*, and vague or template language is unlikely to be acceptable.

GDPR Article 28 Provisions

GDPR Article 28 sets out the minimum requirements that a controller must impose on a processor when outsourcing or subcontracting personal data processing activities, including implementing a contract that defines the scope of the personal data processing and imposing certain requirements on the processor (see Practice Note, Data Processor Obligations Under the GDPR).

Where the controller-to-processor or processor-to-processor modules are used, the New Transfer SSCs incorporate provisions to enable an organization to comply with their GDPR Article 28 obligations. For example, for controller-to-processor transfers, Clause 9 of the New Transfer SCCs provides options either for specific prior authorization or general written authorization for the engagement of sub-processors and a requirement to impose the same data protection obligations on any sub-processors (Article 28(2), (4), GDPR). Although removing the need to negotiate two different agreements simultaneously, it may also reduce an organization's ability to negotiate the nuances of these provisions. For example, processors may want to avoid stricter contractual provisions, particularly in an intra-group context, or limit a controller's ability to conduct audits by including notice requirements or by stipulating that information provided will be limited to what is reasonably necessary. Similarly, controllers often negotiate stricter provisions, for example, requiring processors to provide immediate rather than prompt notification of a data subject rights request. As the New Transfer SCCs explicitly include these provisions, organizations will need to make stronger arguments to deviate from them, be able to justify them, and confirm to a supervisory authority that they do not conflict with the New Transfer SCCs in the event of an investigation.

For more on the Article 28 SCCs, see Article, Key Takeaways from the European Commission's Article 28 Standard Contractual Clauses.

Docking Clause

The optional docking clause allows parties to join as signatories after execution of the New Transfer SCCs by completing a new data transfer appendix, if all parties agree (Clause 7, New Transfer SCCs). The docking clause provides the mechanism for accession. However, it is unclear how existing parties would give agreement. Organizations should consider how to operationalize this, for example, by an accession letter and a process for obtaining the agreement of all existing group company signatories.

The New Transfer SCCs offer a practical solution for multinational organizations reliant on SCCs for their intra-group transfers. These organizations often hold personal data in centralized databases or make regular transfers of employee and consumer data between entities in different countries. Implementing separate SCCs for each intra-group transfer is impractical and often impossible in these scenarios, and accession to an existing agreement offers a practical solution.

Amendment of the New Transfer SCCs

The New Transfer SCCs are standard clauses approved by the European Commission and cannot be amended in a material way. For example, organizations cannot negotiate to remove particular contractual obligations or lower the standard of protection offered. However, the New Transfer SCCs do permit the introduction of other clauses or additional safeguards, if any additions do not:

- Contradict, directly or indirectly, the New Transfer SCCs.
- Prejudice data subjects' fundamental rights or freedoms.

(Clause 2, New Transfer SCCs.)

The New Transfer SCCs actively encourage the inclusion of additional contractual commitments that supplement the New Transfer SCCs' provisions, in line with the *Schrems II* decision (Recital 3, New Transfer SCCs).

Organizations can incorporate the New Transfer SCCs into a wider contract. Organizations may prefer to separate the New Transfer SCCs from any commercial terms, for example, by including the New Transfer SCCs in an appendix, considering that data subjects may request a copy of the completed New Transfer SCCs and a supervisory authority may also request access to the New Transfer SCCs.

Where there is a conflict between the New Transfer SCCs' provisions and the provisions of related agreements between the parties, the New Transfer SCCs must prevail (Clause 5, New Transfer SCCs).

There is no guidance on what additional provisions would be considered contradictory to the New Transfer SCCs' provisions. Provisions lowering the standard of personal data protection would likely be considered contradictory since it would undermine the aim of the New Transfer SCCs. The European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Supplementary Measures Recommendations) provides examples of supplementary contractual provisions that organizations may consider adding to the New Transfer SCCs, including:

- Additional transparency obligations.
- Obligations to inform the data exporter if the data importer is no longer able to provide sufficient protection.

- Enhanced powers to audit the data importer.

(Supplementary Measures Recommendations, at 37 to 40.)

These kinds of provisions would likely not contradict the New Transfer SCCs because they reinforce and enhance the standard of protection offered.

Attempts to allocate risks and liabilities are common under data processing agreements given the potential costs of GDPR personal data breaches or enforcement. In the absence of substantive guidance, it is unclear how attempts to allocate costs and liabilities between the parties or provisions that do not directly lower the SCCs' level of protection but provide a different and contradictory type or level of protection would be viewed. If the amendment does not limit liability regarding a data subject or weaken the rights of affected data subjects both under law and under the New Transfer SCCs, these amendments may be regarded as a commercial issue. Further guidance on this topic is needed.

Impact of *Schrems II*

The New Transfer SCCs include new provisions that are influenced by the *Schrems II* decision and are relevant to all four modules (Section III, New Transfer SCCs).

Third Country Assessments and Analysis of Data Transfer Risks

The New Transfer SCCs require the parties to perform and document their assessment of the destination country's law and practices for all transfers relying on the New Transfer SCCs and make them available to the competent supervisory authority on request. The data importer is primarily responsible for performing this assessment. However, both parties must warrant that they have no reason to believe that applicable laws and practices in the destination country would prevent the data importer from fulfilling its obligations under the New Transfer SCCs. The parties must consider certain factors in giving this warranty, including:

- The circumstances of the transfer, including the number of parties involved and transmission channels used, intended onward transfers, recipient type, the processing purpose, categories and format of data, the relevant sector in which the parties operate, and the storage location of the transferred data.
- The parties' practical experience of public authority access to data, if this is supported by other relevant, objective elements, including publicly accessible and reliable information.
- The extent to which the laws and practices in the destination country permit public authorities to access data, as relevant to the specific transfer circumstances and applicable limitations and safeguards.
- Any relevant contractual, technical, or organizational safeguards that supplement the New Transfer SCCs.

(Clause 14, New Transfer SCCs.)

The data importer must notify the data exporter of changes that affect its ability to comply with the New Transfer SCCs, in particular, its ability to prevent public authority access to data, so that the data exporter can implement supplementary measures or suspend the transfers if it is not possible to implement appropriate supplementary measures.

The New Transfer SCCs also address onward transfers and the requirements to perform a transfer impact assessment and apply appropriate safeguards to onward transfers. The New Transfer SCCs require data importers acting as a

controller to notify data subjects of specific details about onward transfers, including the transfer purpose and the legal basis for the transfer.

For more on third country assessments, see Articles, EDPB Supplementary Measures Recommendations and German DPA Guidance Post Schrems II and Schrems II: FISA and EO 12333 Overview.

Obligations Concerning Public Authority Access Requests

Where a data importer receives a public authority request for data or becomes aware of direct access to data by a public authority, the data importer must:

- Promptly notify the data exporter and, where possible, the affected data subjects. If the public authority prohibits the data importer from notifying the data exporter or data subject, the data importer must use its best efforts to obtain a waiver of the prohibition.
- Review the legality of and challenge access requests, to the extent possible. The data importer must minimize the data provided in response to any request and document its assessment of potential challenges to a government request and its efforts to challenge the request. Data importers must also provide regular reports on requests from public authorities.

(Clause 15, New Transfer SCCs.)

These obligations are significantly more onerous than those imposed in the context of transfers before the *Schrems II* decision, particularly for data importers, who are now required to play an active role in establishing that their own country's laws enable them to provide an EU equivalent standard of data protection. Data importers must undertake thorough risk assessments both internally and regarding external factors and provide evidence to data exporters of their ability to protect data, particularly against access from government agencies. The existing SCCs were viewed by many organizations as a box ticking exercise before *Schrems II*. However, the New Transfer SCCs impose a significant compliance burden that requires research, judgment, documentation, and a considerable degree of cooperation between data exporters and data importers that previously may have been limited to agreeing to liability provisions.

The ongoing nature of these obligations also requires data importers to ensure that they implement a procedure to remain up-to-date on laws and governmental practices that may affect their ability to comply. Data exporters will also need to implement their own procedures to ensure consistency in the jurisdictions that are considered safe to export personal data to and must remain agile if a particular jurisdiction or data importer becomes unsafe due to a change in law or practice and must be replaced. These policies and procedures should focus on identifying, challenging, responding to, and documenting access requests and how the organization will cooperate with other relevant parties on those matters. Some organizations may consider adopting policies directed at providing greater transparency to data subjects regarding any requests received. Organizations should also update their vendor onboarding and diligence procedures to ensure that relevant issues are addressed in the onboarding process.

Security

The New Transfer SCCs impose new obligations on data exporters and data importers, such as a requirement for the data importer to perform regular checks to ensure that its security measures continue to provide an appropriate level of security. The New Transfer SCCs also contain additional detail concerning the security measures that may be implemented, such as encryption or pseudonymization during transmission. Where the data importer acts as a processor, the New Transfer SCCs specify that the data exporter should retain control of information required to re-identify the data.

Third-Party Beneficiary Rights

The Recitals to the existing SCCs required the existing SCCs to be governed by a law that enabled the enforcement of third-party beneficiary rights. The New Transfer SCCs explicitly include this requirement in the operative provisions of the New Transfer SCCs (Clause 17, New Transfer SCCs). The UK and all EU member states recognize third-party beneficiary rights.

Clause 3 of the New Transfer SCCs permits relevant provisions to be enforced directly against both data exporters and data importers, while the existing SCCs only permitted direct enforcement of these rights against the data exporter. Data importers must inform data subjects of an easily accessible contact point and deal promptly with any data subject complaints or requests (Recital 12 and Clause 11(a), New Transfer SCCs). In the controller-to-controller, controller-to-processor, and processor-to-processor modules, the New Transfer SCCs permit an individual to lodge a complaint with the relevant supervisory authority or refer the dispute to a competent EU court, and the data importer must agree to accept a binding decision under EU or member state law (Clause 11, New Transfer SCCs).

The *Schrems II* decision highlighted the lack of actionable rights for individuals before a body offering guarantees substantially equivalent to those required under EU law as a reason for invalidating the Privacy Shield. The New Transfer SCCs bolster EU data subject rights through these additional requirements. Depending on the nature of the data transfers and associated risks in question, some organizations may want to grant additional third-party beneficiary rights regarding additional contractual safeguards included in the agreement that go beyond those included in the New Transfer SCCs.

Data Transfers from the UK

The New Transfer SCCs have not been adopted for use in the UK, and the transition periods above do not apply to personal data transfers from the UK. The New Transfer SCCs were adopted under the GDPR after the date of the UK's withdrawal from the EU. The New Transfer SCCs do not form part of retained EU law under UK domestic law. UK organizations cannot use the New Transfer SCCs for data transfers from the UK and must continue to use the existing SCCs. Where existing SCCs are used, the ICO has indicated that limited changes may be made so they make sense in a UK context, if the substantive provisions of the existing SCCs are not changed. For example, changing "EU Member States" to "the UK" and "supervisory authorities" to "the ICO" is permitted. The ICO has published a modified version of the existing SCCs for UK data transfers (see ICO: Guide to the UK GDPR: Standard Contractual Clauses (SCCs) after the transition period ends).

On August 11, 2021, the ICO published for public consultation until October 7, 2021:

- A draft international data transfer agreement for UK data transfers (essentially the UK equivalent of the New Transfer SCCs).
- A draft data transfer risk assessment tool.
- A draft UK Addendum to the New Transfer SCCs.
- Updated international data transfer guidance.

(See Legal Update, ICO consults on updated guidance and draft ICO international data transfer agreement for personal data transfers outside UK.)

In May 2021, ICO Deputy Commissioner Steve Wood said that the ICO is "considering the value to the UK for us to recognize transfer tools from other countries, so standard data transfer agreements, so that would include the EU's standard contractual clauses as well."

Where a transaction involves both UK and EU transfers (for example, an intra-group transfer mechanism), the contract will need to incorporate both the New Transfer SCCs for EU transfers and, for now, the existing SCCs for UK transfers. Organizations are likely to wait until the new UK SCCs are finalized before transitioning to the New Transfer SCCs so that the exercise of updating their transfer mechanism is undertaken once. The data transfer addenda are likely to be lengthy once both EU and UK transfer mechanisms are incorporated. For more on the impact of the New Transfer SCCs for UK organizations, see Article, European Commission's new standard contractual clauses: what they mean for UK businesses.

Data Transfers from Switzerland

As Switzerland is not an EU member state, the invalidation of the EU-US Privacy Shield did not automatically invalidate the Swiss-US Privacy Shield. However, on September 8, 2020, the Federal Data Protection and Information Commissioner (FDPIC) confirmed in a position statement that it did not consider the Swiss-US Privacy Shield adequate for personal data transfers from Switzerland to the US. Swiss organizations are therefore heavily reliant on SCCs for personal data transfers from Switzerland.

The FDPIC recognized the existing SCCs as providing sufficient protection for transfers. However, the New Transfer SCCs do not automatically apply in Switzerland. The FDPIC indicated that it intends to approve the New Transfer SCCs for use by Swiss data exporters. It is unclear whether the existing SCCs will remain valid and if there will be a transition period as in the EU.

Next Steps

Organizations should:

- Perform a thorough data mapping exercise to identify every transfer involving EU or UK personal data, including transfers of personal data collected directly from EU or UK data subjects, for example, by organizations subject to GDPR Article 3(2). This should cover both intra-group and external data transfers.
- Prioritize data transfers based on risk to individuals. Countries with less comprehensive data protection laws than the EU or where public authority access to data is more likely should be considered high risk. Prioritize business critical transfers that would cause significant disruption if suspended.
- Identify whether SCCs are currently or should be used for each transfer or whether any other transfer mechanisms may apply. If the SCCs apply, establish the capacity in which the parties are acting for each transfer and agree on this with the other party, as both will need to agree on which New Transfer SCC module applies to the relevant transfer before execution.
- Monitor progress of the ICO's consultation on its draft international data transfer agreement, UK Addendum to the New Transfer SCCs, risk assessment, and updated guidance on cross-border data transfers (see Practice Note, UK data protection regime: regulatory guidance and consultations).
- Understand the obligations imposed under the New Transfer SCCs. Assess if new policies and procedures should be implemented to assess the level of risk to personal data in the exporting and importing countries, including the potential for public authority access to personal data.

- Review and understand the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and the issues highlighted in the *Schrems II* decision when undertaking transfer impact assessments. Monitor guidance from relevant supervisory authorities as it develops (see Practice Notes, EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker, GDPR Data Protection Authority Guidance Tracker by Country (EEA), and GDPR European Data Protection Board Guidance Tracker).
- Consider any supplementary measures to mitigate any identified risks and agree on them with the other parties. Ensure any processes or procedures are appropriately documented and monitored to meet the parties' accountability obligations.

Data importers will also need to perform these steps for any onward transfers of data.

END OF DOCUMENT

