Data Protection & Information Security Working Group - International Data Transfers and Standard Contractual Clauses - Latest EU and UK Developments

Author: Flavien Corolleur,
Senior Legal Counsel/Director and Data Protection Officer at SS&C Financial Services (Ireland) Limited and member of the Compliance Institute's DP&IS Working Group.

On 4 June 2021, the European Commission published a decision in respect of a new set of modernised standard contractual clauses ("EU SCCs")[1] for compliance purposes with the EU General Data Protection Regulation ("GDPR"), taking into account the decision from the Court of Justice of the European Union ("CJEU") published on 16 July 2020[2] in connection with the EU-US Privacy Shield and the old standard contractual clauses ("Old SCCs") ("Schrems II Decision")[3].

With 6 months only to the deadline of 27 December 2022 to repaper the Old SCCs with the new EU SCCs, this article will give an overview of some of the key steps to undertake when implementing these new EU SCCs. This article will then look at some of the developments over the last 12 months, including the new template agreements published by the UK supervisory authority, the Information Commissioner's Office ("ICO"), to address data transfers from the UK to third countries. Thirdly, this article will highlight some forthcoming developments.

The Clock Is Ticking: 6 Months to the 27 December 2022 Deadline to Repaper Old SCCs with the New EU SCCs!

Before considering some of the key steps to undertake in implementing the new EU SCCs, we will give a brief overview of the EU SCCs construct.

- **A brief overview of the EU SCCs**

The EU SCCs consist of four main sections and three annexes.

The **first general section** (1) describes the purpose and scope of the EU SCCs, (2) clarifies which terms of the EU SCCs may be invoked and enforced by data subjects as third party beneficiaries, (3) indicates any terms used in the EU SCCs have the meaning given to them under GDPR, (4) clarifies the EU SCCs terms will prevail should there be any conflict with any other agreement the parties to the EU SCCs may have entered into and (5) describes the transfer. In addition, the first general section includes an optional clause (the "**docking clause**"), according to which the parties to the EU SCCs may wish to add a third party either as a data exporter or data importer by completing and signing Annex A.1.

The **second section, specific to the parties' obligations,** adopts a "**modular approach**" and offers four options, depending on the type of processing and parties associated with such processing. The four modules of the EU SCCs are:

- (1) controller to controller (C2C),
- (2) controller to processor (C2P),
- (3) processor to processor (P2P); and
- (4) processor to controller (P2C).

The modular approach applies to both the basic terms regarding data protection safeguards (such as accuracy and data minimisation, storage limitation, security of processing and reporting of a data breach) and provisions in connection with local laws, which may affect compliance with the EU SCCs, including the use of sub-processors and liability terms.

The **third section of the EU SCCs** relates to the local laws and obligations governing access by public authorities. In particular, the parties to the EU SCCs must conduct and document an assessment in connection with the laws and practices in the third country of destination applicable to the processing of personal data.

The **fourth section of the EU SCCs** features **various general provisions,** including, for instance, the obligation on the data importer to promptly inform the data exporter if it is unable to comply with the EU SCCs. Furthermore, EU SCCs should be governed by the laws of an EU Member State, provided that such laws allow for third-party beneficiary rights.

Lastly, the EU SCCs include **three annexes**, namely to describe (1) the list of **parties**, the **type of transfer** and **competent authority**, (2) the **technical and organisational measures** agreed upon between the parties and (3) the **list of sub-processors**.

- **Other considerations?**

On 25 May 2022, the European Commission published a **Q&A[4] to the new EU SCCs** to address in 44 questions feedback from various stakeholders on their experience using the latest EU SCCs since their adoption in June 2021. The Q&A is intended to be "dynamic" and may be updated as new questions arise. Some of the important questions addressed include questions such as whether the parties to the EU SCCs may add additional clauses to the EU SCCs or incorporate the EU SCCs into a broader commercial contract. Other questions relate to whether the liability under the EU SCCs can be limited by general liability clause in the main commercial agreement.

In this respect, the parties to the EU SCCs are free to include the EU SCCs in a wider contract, namely the primary commercial agreement between the parties. In addition, while the data exporter and data importer may not amend the terms set out in the EU SCCs, the parties may add other clauses or additional safeguards "*provided that they do not contradict, directly or indirectly, the (SCCs) or prejudice the fundamental rights or freedoms of data subjects*." The Q&A also clarifies that the liability clauses of the EU SCCs **do not affect the liability provisions that may apply to other aspects** to the contractual relationship between the parties.

- **Some of the key implementation steps include:**

1. Determine which parties are processor and/or controller, respectively

On 7 July 2021, the EDPB adopted the updated Guidelines 07/2020 Version 2.0 on the concepts of controller and processor in the GDPR[5]. These important Guidelines provide guidance on the concepts of controller and processor with concrete examples concerning these concepts.

When selecting the relevant module (C2C), (C2P), (P2P), or (P2C) for the purpose of the EU SCCs, a careful review of the above Guidelines would be expected to ensure the relevant parties are correctly identified as either controller and/or the processor.

2. Conduct and document a transfer impact assessment ("TIA")

The parties to the EU SCCs, amongst other things, must warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under the EU SCCs.

It means that the parties to the EU SCCs must conduct a TIA of the relevant laws and practices of the third

country. Furthermore, the risk-based assessment of the laws and practices of the third country of destination must be documented and made available to the competent data protection authority upon request.

3. Implement and document supplementary measures

On 18 June 2021, the European Data Protection Board ("EDPB")[6] adopted the final version of the recommendations on measures supplementing transfer tools to ensure compliance with the EU level of protection of personal data Supplementary Safeguards Measures[7] ("Recommendations"). The Recommendations are meant to assist exporters in assessing third countries and identifying the appropriate supplementary measures to be implemented before transferring personal data to such third countries. To that effect, the Recommendations provide a series of steps to follow, a potential source of information and some examples of supplementary measures that may be put in place.

With respect to assessing the law of a third country, the Recommendations refer to the European Essential Guarantees for surveillance measures recommendations adopted by the EDPB on 10 November 2020[8]. The assessment of the legislation of the third country of destination should be based on "objective factors" regardless of the likelihood of access to personal data. Objective factors include aspects such as (a) the purposes for which the data are transferred and processed (e.g., marketing, HR, storage, IT support), (b) the types of entities involved in the processing (public/private), (c) the sector in which the transfer occurs (e.g., telecommunication, financial), (d) the categories of personal data transferred and, (e) the format of the data transferred (i.e., in plain text, pseudonymised or encrypted).
Another important point highlighted in the Recommendations is that exporters are expected to re-evaluate at appropriate intervals the level of protection afforded to the personal data transferred to third countries. In addition, exporters should monitor if there have been or there will be any developments that may affect such protection.

4. Engage without further delay with both clients and vendors to implement both the EU SCCs and requisite provisions under Article 28.3 of GDPR if not already done.

One of the benefits of the EU SCCs is that they incorporate the Article 28.3 provisions required in data protection agreements between controllers and processors. Implementing the new EU SCCs will therefore remedy any old data protection arrangements that may not comply with GDPR.

In respect of the Article 28.3 requisite provisions between controllers and processors, the French data protection authority (CNIL) imposed on a French data processor in April 2022 an administrative fine of 1.5 million euros on the basis, among other things, that the general terms and conditions and related agreements proposed by the processor to its clients did not contain the mentions provided for in Article 28-3 of GDPR9.

5. Ensure you have a process to provide a copy of the new EU SCCs to a data subject upon request.

On request, the parties to the EU SCCs need to make a copy of the EU SCCs, including the annexes available to the data subject, free of charge. While the parties may redact part of the text of the annexes before sharing a copy to protect business secrets or other confidential information, they should (1) provide a "meaningful summary" where the data subject would otherwise not be able to understand its content or exercise their rights and (2) on request, provide the data subject with the reasons for the redactions "to the extent possible without revealing the redacted information."

Irish Companies with Affiliates in Other Jurisdictions: UK and Swiss Requirements

- **UK new international data transfer agreement ("IDTA") and addendum to EU SCCs ("UK Addendum")**

On 21 March 2022, a set of documents, including the IDTA, UK Addendum and a document setting out transitional provisions issued by the ICO, was approved by the UK Parliament[10].

A Brief Overview and Guidance in relation to the IDTA, Addendum

The IDTA and UK Addendum replace Old SCCs for international transfers, taking into account the CJEU Schrems II Decision. UK exporters can use the IDTA or the UK Addendum as a transfer tool to comply with Article 46 of the UK GDPR when making restricted transfers. The IDTA is meant to be the equivalent to the new EU SCCs. The purpose of the UK Addendum is to amend the new EU SCCs to work in the context of UK data transfers to third countries.

The ICO is expected to publish some time soon further guidance, including (i) clause by clause guidance to the IDTA and UK Addendum, (ii) guidance on how to use the IDTA, (iii) guidance on transfer risk assessments and (iv) further clarifications on its international transfers guidance.

How much time do we have?

- Transfer arrangements using the Old SCCs put in place prior to 21 September 2022 are expected to remain valid until 21 March 2024, subject to no changes to the underlying processing.

- From **21 September 2022**, UK companies must use the IDTA or the UK Addendum for any new transfers to third countries.

UK addendum or IDTA: which one to choose? A question of pragmatism, but consider the implementation deadlines

	UK Addendum to new EU SCCs	IDTA
Deadline to implement	27 December 2022 (together with new EU SCCs)	21 March 2024
Overview	Short easy to use document, supplement new EU SCCs to make them work for UK GDPR compliance	Similar in principle to new EU SCCs, yet pragmatic and business-friendly document
Modular approach?	Yes, new EU SCCs, which the UK Addendum will refer to, cover C2C, C2P, P2P and P2C.	No. IDTA refers to linked agreement" which will need to address controller / /processor requirements if the importer is a processor or sub-processor
Article 28.3 UK GDPR included?	Yes, new EU SCCs, to which UK Addendum will refer, already includes Article 28.3 GDPR requirements	No. Article 28.3 of UK GDPR will need to be addressed in a separate agreement.
Can they be amended?	No, but exporter and importer may add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the [SCCs] or prejudice the fundamental rights or freedoms of data subjects.	No, but exporter and importer may include provisions in a "linked agreement" to provide enhanced rights otherwise covered by IDTA or commercial terms, including payment. Still, these commercial terms should not affect the rights granted under IDTA.
Is a TIA required?	Yes	Yes
Anything else?	The UK Addendum can only be used with the new EU SCCs, i.e., not with other clauses that may be published by other countries.	Monitor and consider the further guidance expected to be published by the ICO.

- **Swiss: pragmatic approach in recognising EU SCCs subject to certain requisite changes**

On 27 August 2021, the Swiss data protection authority (Federal Data Protection and Information Commissioner or "FDPIC") published a statement confirming that the FDPIC recognised the EU SCCs for the transfer of personal data from Switzerland to third countries as the basis for personal data transfers to a country without an adequate level of data protection, subject to necessary adaptations and amendments.

To that effect, the FDPIC statement includes a helpful table outlining the adaptations to be made to the EU SCCs necessary for compliance with Swiss data protection law.

With respect to determining the law governing the SCCs (i.e., EU versus Switzerland), the FDPIC statement also includes some helpful guidance regarding the options the parties to the SCCs may consider when the data transfers are subject to both GDPR and Swiss data protection law.

Other Forthcoming Developments?

- **Brace yourself: forthcoming EU SCCs for Art. 3 GDPR companies**

As indicated by the EDPB in the minutes of its plenary meeting of 14 September 2021, a draft "Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR"[11] was published for public consultation, with comments expected by 31 January 2022.

In order to assess whether the processing of personal data to a third country is deemed a "transfer" for the purpose of Chapter V of GDPR, resulting potentially in the controller/processor being required to implement one of the instruments set out under GDPR (such as standard contractual clauses, binding corporate rules), the EDPB has identified three cumulative criteria that qualify the processing as a "transfer":

1. Controller or processor is subject to GDPR for the given processing,

Controller or processor (exporter) discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor (importer), and

2. The importer is in a third country or is an international organisation, irrespective of whether this importer is subject to the GDPR of the given processing in accordance with Article 3 of GDPR.

3. The draft guidelines include seven practical examples of whether such processing is or is not, a "transfer," and a section headed "consequences," including a summary.

- **The revival of the Privacy Shield: US and EU political engagement for a forthcoming EU/US Trans-Atlantic Data Privacy Framework**

Twenty months after the Schrems II Decision, President Biden and European Commission President Ursula von der Leyen gave a joint US-EU press statement on 25 March 2022 regarding a Trans-Atlantic Data Privacy Framework.

The new Trans-Atlantic Data Privacy Framework, expected potentially before the end of 2022, should ensure, among other things, that:

- Intelligence collection of personal data may be undertaken only where necessary to advance legitimate national security objectives and must not disproportionately impact the protection of individual privacy and civil liberties;

- EU individuals may seek redress according to a new multi-layer redress mechanism that includes an independent Data Protection Review Court that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed; and

- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

REFERENCES:

1 https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf
2 Decision C311/18 Irish Data Protection Commissioner v Facebook Ireland Limited. In this decision, the CJEU invalidated the EU-US Privacy Shield, yet it also confirmed the SCCs remained valid.
3 The "old" standard contractual clauses are the clauses set out in the Decisions 2001/497/EC and 2010/87/EU for the transfer of personal data to third countries and processors established in such countries under the Data Protection Directive 95/46/EC
4 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
5 https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
6 The EDPB is an independent European body composed of the EU national data protection authorities which, amongst other things, provides general guidance to clarify the law and to promote a common understanding of EU data protection laws
7 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
8 https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
9 https://www.cnil.fr/en/health-data-breach-dedalus-biologie-fined-15-million-euros#:~:text=On%2015th%20April%202022%2C%20the,concerning%20nearly%20500%20000%20individuals.
10 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/
11 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en