Understanding the European Commission's New Standard Contractual Clauses for Transfer of Personal Data from EU to Non-EU Regions

Frequently Asked Questions & Answers

The European Commission adopted a new set of Standard Contractual Clauses for the transfer of personal data to non-EU regions ("**New SCCs**"), which came into effect on 27 June 2021. The New SCCs take account of the requirements of the General Data Protection Regulation ("**GDPR**") and the judgment of the Court of Justice of the European Union ("**CJEU**") in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18 (commonly known as the "***Schrems II* Judgment**").

The New SCCs will be relevant to a local entity in Hong Kong if the obligations under the GDPR apply to it as an exporting party on an extra-territorial basis. For instance, the requirements of the GDPR apply even though a Hong Kong entity does not have an establishment in the European Union ("**EU**")/European Economic Area ("**EEA**")[1] so long as its data processing activities are related to the offering of goods or services to, or the monitoring of the behaviour of individuals in the EU/EEA. For Hong Kong entities which are not subject to the GDPR but import EU/EEA personal data, they may also be required to adopt the New SCCs when entering into data transfer agreements, and submit themselves to the jurisdiction of the data protection supervisory authorities identified therein (Clause 13(b)).

This set of Frequently Asked Questions & Answers examines from a practical perspective the implementation framework of the New SCCs and the obligations of parties entering into cross-border data transfer agreements consisting of the New SCCs. For any relevant issue about the applicability of the GDPR and further questions arising from the adoption of the New SCCs in data transfer agreements, local entities should also consult their own legal advisers or the data protection authority(ies) concerned where appropriate.

Part I: The Overall Application of the New SCCs

[1] The Agreement on the European Economic Area ("**EEA Agreement**") provides for the extension of the EU's internal market to the three EEA States Iceland, Liechtenstein and Norway. The GDPR is covered by the EEA Agreement and applies to the EEA.

Q1. What types of data transfer do the New SCCs cover?

A: The New SCCs, in substitution for the controller-to-controller and controller-to-processor standard contractual clauses that were previously adopted under the then Data Protection Directive 95/46/EC ("**Old SCCs**"), cover transfer of personal data from the EU/EEA to a non-EU region where its data protection laws have not been recognised by the European Commission as offering adequate data protection[2].

A modular approach is adopted in the New SCCs where different combinations of clauses are devised to enable four types of transfer as follows:

(i) From a controller to another controller (C2C);

(ii) From a controller to a processor (C2P);

(iii) From a processor to another processor (P2P); and

(iv) From a processor to its appointing controller (P2C).

Q2. Who can rely on the New SCCs?

A: The New SCCs are applicable in cases where a data exporter is subject to the GDPR but the data importer is not. If a data exporter is not established in the EU/EEA but is subject to the GDPR on an extra-territorial basis, it may rely on the New SCCs for transfer of EU/EEA personal data to non-EU regions so long as its data processing activities fall under Article 3(2) of the GDPR[3].

It follows that a local company may be required to adopt the New SCCs under the circumstances where it acts a data importer receiving EU/EEA personal data.

[2] The New SCCs will replace and repeal the SCCs adopted by the European Commission in 2001 (and subsequently amended in 2004) and 2010, for transfer of personal data to controllers and processors in non-EU regions respectively, under the then Data Protection Directive 95/46/EC.

[3] Article 3(2) of the GDPR sets out the conditions under which the GDPR applies to the processing activities of a data controller/processor not established in the EU. It stipulates that:
"*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

In addition, the New SCCs will be applicable to a local entity which acts as a data exporter; and when its data processing activities are subject to the GDPR under Article 3(2) thereof on an extra-territorial basis (such as when its data processing activities are related to the offering of goods or services to individuals in the EU/EEA, etc.).

Examples of Hong Kong organisations which may be subject to the New SCCs include (the following list is not exhaustive):

(i) Hong Kong organisations with businesses or operations in the EU/EEA which transfer personal data to elsewhere;

(ii) Hong Kong data controllers which import EU/EEA personal data from another data controller being subject to the GDPR; and

(iii) Hong Kong organisations which import EU/EEA personal data as data processors.

Q3. Is there any transitional period for data exporters and importers to adopt the New SCCs?

A: Data exporters and importers may still opt to conclude a contract incorporating the Old SCCs until 27 September 2021.

Meanwhile, organisations are given a transitional period of 18 months from the date when the New SCCs became effective (i.e., from 27 June 2021 to 27 December 2022) to replace all existing contracts containing the Old SCCs with the New SCCs, provided that the processing operations being the subject matter of the contractual agreement remain unchanged and that the transfer of personal data is subject to appropriate safeguards.

Q4. Is it possible for additional parties to sign a contractual agreement incorporating the New SCCs after it has been executed by the existing parties in the first place?

A: The introduction of an optional docking clause in the New SCCs (i.e., Clause 7) allows an entity that is not a party to the agreement at the time of its execution to accede to the clauses thereof at any time, upon the agreement of the existing parties.

Q5. Do parties have to incorporate the data security measures implemented in the New SCCs?

A: Parties to the New SCCs are required to set out the technical and organisational measures adopted to safeguard the personal data transfer in question in specific terms (such as pseudonymisation and encryption of personal data, measures for protection of data during transmission, etc.) in Annex II of the New SCCs ("*Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data*"). Further, particulars as to which measures apply to each transfer/set of transfers have to be provided with clarity therein.

Q6. What is the significance of the *Schrems II* Judgment in bringing about the adoption of the New SCCs?

A: In the *Schrems II* Judgment, the CJEU struck down the framework of the EU-US Privacy Shield[4] while reiterating that the Old SCCs enabling the transfer of personal data outside of the EU were still valid.

The CJEU declared the EU-US Privacy Shield invalid as it considered that a level of protection essentially equivalent to that required by the GDPR could not be afforded to EU citizens when read in light of the EU Charter of Fundamental Rights ("**Charter**") for the respect of private and family life, personal data protection and the right to effective judicial protection. The CJEU observed that the statutory provisions and rules on surveillance programmes of the United States ("**US**") did not indicate clear limitations on the powers that they conferred to implement those programmes, or the existence of guarantees targeted at non-US persons and hence being contrary to the principle of proportionality concerning interference with fundamental rights. The CJEU further observed that EU citizens were not given actionable rights before the Courts against the US authorities. The lack of effective judicial protection for EU data subjects further led to the invalidation of the Privacy Shield by the CJEU.

[4] The EU-US Privacy Shield was formulated to facilitate transatlantic transfer of personal data from the EU to the US, after the CJEU had invalidated the US-EU Safe Harbour Framework (in Case C362-14, commonly known as the "***Schrems I* Judgment**") in October 2015.

In contrast, the CJEU considered that the Old SCCs formulated in the pre-GDPR era, when viewed from the perspective of the GDPR concerning appropriate safeguards, enforceable rights, effective legal remedies, and the Charter in particular, still offered an adequate level of protection to the individuals as required under the GDPR. Nevertheless, the underlying transfer must be assessed on a "case-by-case" basis in ensuring that the level of protection guaranteed by the GDPR would not be undermined. The CJEU stressed that an assessment of the appropriate level of protection required looking into (i) the contractual clauses agreed between the data exporter in the EU and the recipient of the personal data in the non-EU region; and (ii) the possibility of an access by the public authorities of the non-EU region to the data transferred on the grounds of national security and more (including the relevant aspects of the legal system of that non-EU region).

To this end, clauses formulated in response to the *Schrems II* Judgment (such as in relation to access of personal data by public authorities, etc.) were incorporated in the New SCCs.

Q7. How should parties to the New SCCs assess the impact of transferring personal data to any non-EU region of destination?

A: Clause 14 requires the parties to conduct an assessment of the laws and practices in the non-EU region to which the personal data are transferred which are applicable to the processing of personal data by the data importer, including any requirements or measures in respect of which public authorities will have access to the personal data concerned.

The parties have to warrant that they have no reason to believe that the relevant laws and practices in the destination of transfer prevent the data importer from fulfilling its obligations under the New SCCs, upon consideration of the relevant factors below:

(i) The circumstances of the subject data transfer, such as the length of the processing chain, the purpose of processing, the storage location of the data transferred, etc.;

(ii) The laws and practices of the non-EU region of destination, including any requirement under which the subject personal data are disclosed to public authorities or the public authorities' access to such personal data is authorised, the applicable limitations and safeguards; and

(iii) Any relevant safeguards put in place in addition to safeguards provided under the New SCCs.

Once the data importer has reason to believe that it is or has become subject to the relevant laws or practices in the non-EU region which are not consistent with its warranty previously made, it shall notify the data exporter promptly. The data exporter shall then identify appropriate measures to be adopted to address the situation. The data transfer in question shall be suspended if the data exporter considers that no appropriate safeguards can be ensured for such transfer or as instructed by the competent supervisory authority[5] concerned. The contract governing the data transfer in question may also be terminated under such circumstances.

Q8. What are the obligations of a data importer when public authorities in the destination of transfer request access to the personal data concerned?

A: A data importer agrees to do the following in such circumstances pursuant to Clause 15 of the New SCCs:

(i) To notify the data exporter and, where possible, the data subject promptly of the access request from a public authority or any actual access by the public authority;

(ii) To provide the data exporter with as much relevant information as possible regarding access requests received on a regular basis;

(iii) To make the information regarding the access requests received and any actual access by the public authority available to the competent supervisory authority concerned on request;

[5] A competent supervisory authority is the data protection supervisory authority identified by the parties in Clause 13(a) of the New SCCs, which is responsible for ensuring compliance with the GDPR by the data exporter. The data importer also agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with the New SCCs (Clause 13(b)).

(iv) To review the legality of the request for disclosure, and to challenge the request if it concludes that there are reasonable grounds to consider the request unlawful after careful assessment of the relevant factors;

(v) To pursue possibilities of appeal where appropriate;

(vi) To document its legal assessment and any challenge to the request for disclosure; and

(vii) To provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Q9. Can data subjects invoke and enforce the New SCCs?

A: Clause 3(a) provides that data subjects may invoke and enforce the majority of the provisions in the New SCCs as third-party beneficiaries against the data exporter(s) and/or data importer(s). The only exceptions to this are, *inter alia*, the clauses that touch upon the rights and obligations of the parties which are to be observed among the data exporters and data importers themselves, etc.

Q10. What is the apportionment of liability to data subjects among parties to the New SCCs in data breach incidents?

A: Reference is made to Clause 12 of the New SCCs. In this regard, Clause 12(c) for transfer from a controller to another controller and transfer from a processor to its appointing controller; and Clause 12(e) for transfer from a controller to a processor and transfer from a processor to another processor provide that all the responsible parties shall be jointly and severally liable for any damage caused to the data subject as a result of a breach of the clauses. The data subject is entitled to bring an action in court against any of the parties.

Further, a party which is held liable shall be entitled to claim back from the other party(ies) the part of compensation corresponding to the responsibility of the latter party(ies) for the damage, pursuant to Clause 12(d) for transfer from a controller to another controller and transfer from a processor to its appointing controller; and Clause 12(f) for transfer from a controller to a processor and transfer from a processor to another processor.

Q11. What will happen if a data importer is unable to comply with the New SCCs?

A: In the event that the data importer is in breach of the New SCCs or unable to comply with the same, the data exporter shall suspend the data transfer until compliance is again ensured or the contract is terminated (Clause 16(b)).

The data exporter is entitled to terminate the contract if:

(i) Upon suspension of the data transfer, compliance with the New SCCs is not restored within a reasonable time and in any event within one month of suspension;

(ii) The data importer is in substantial or persistent breach of the New SCCs; or

(iii) The data importer fails to comply with a binding decision of a competent court or a supervisory authority regarding its obligations under the New SCCs (Clause 16(c)).

The personal data that has been transferred prior to the termination of the contract shall be returned or deleted in its entirety (as the case may be). The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure its compliance with the New SCCs (Clause 16(d)).

Q12. What are the governing law, choice of forum and jurisdiction in respect of contractual agreements consisting of the New SCCs?

A: Parties to the New SCCs (under C2C, C2P and P2P) enjoy the flexibility in selecting the governing law (provided that the law allows for third-party beneficiary rights) and choice of jurisdiction of any EU member state in respect of the data transfer agreements (Clauses 17 and 18). For P2C of the New SCCs, the governing law and choice of jurisdiction selected by the parties are not required to be of any EU member state.

Part II: A Closer Look at the Individual Modules under the New SCCs

Q13. Apart from the common obligations imposed on the parties regardless of the module under which the data transfer is to take place, what specific data protection safeguards are required to be put in place under the four different modules?

A: The individual clauses under the New SCCs seek to implement various requirements under the GDPR where appropriate. Some of the overriding obligations as appliable to the four different types of data transfers in terms of data protection safeguards to be adopted by the parties are extracted and outlined in the table below.

	(i) C2C	*(ii) C2P*	*(iii) P2P*	*(iv) P2C*
Warranty	(Clause 8) For data exporter • To warrant that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under the New SCCs.			
Instructions	N/A	(Clause 8.1) For data importer • To process the personal data only on documented instructions from the data exporter.	(Clause 8.1) For data exporter • To make the instructions of its controller available to the data importer prior to processing. • To warrant that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under the EU or Member State law between the controller and the data exporter. For data importer	(Clause 8.1) For data exporter • To process the personal data only on documented instructions from the importer acting as its controller. • To delete all personal data processed and certify to the data importer that it has done so, or return the processed personal data to the importer and delete existing copies after the end of the provision of the processing services (if required).

			• To process the personal data only on documented instructions from the controller and the data exporter.	
Purpose limitation	(Clause 8.1) For data importer • To process the personal data only for the specific purpose(s) of the transfer as set out in the contractual agreement, except under the specified circumstances (e.g., where it has obtained the data subject’s prior consent, etc.).	(Clause 8.2) For data importer • To process the personal data only for the specific purpose(s) of the transfer as set out in the contractual agreement, except on further instructions from the data exporter or the controller (as the case may be).		N/A
Transparency	(Clause 8.2) For data importer To inform data subjects of: • its identity and contact details; • the categories of personal data processed; • the right to obtain a copy of the contractual agreement (with necessary redaction to protect business secrets or other confidential information); and • the recipient or categories of recipients of any intended onward transfer of the data subjects’ personal data, the purpose of such onward transfer and the ground(s).	(Clause 8.3) For data exporter • To provide a copy of the contractual agreement to the data subject on request (with necessary redaction).		N/A

Accuracy and data minimisation	(Clause 8.3) For each party • To ensure that the personal data is accurate and, where necessary, kept up to date. For data importer • To take every reasonable step to ensure that any inaccurate personal data, having regard to the purpose(s) of processing, is erased or rectified without delay. • To ensure that the personal data is limited to what is necessary in relation to the purpose(s) of processing.	N/A	N/A	N/A
Accuracy	N/A	(Clause 8.4) For data importer • To cooperate with the data exporter in erasing or rectifying any inaccurate data received.	(Clause 8.4) For data importer • To cooperate with the data exporter in rectifying or erasing any inaccurate data received.	N/A
Storage limitation	(Clause 8.4) For data importer • To retain the personal data for a period not longer than necessary for the purpose(s) for which it is processed with appropriate technical or organisational measures being put in place.	N/A	N/A	N/A

Duration of processing and erasure or return of data	N/A	(Clause 8.5) For data importer • To process the data only for the specified duration. • To delete all personal data processed and certify to the data exporter that it has done so, or return the processed personal data to the exporter and delete existing copies (if required).	N/A
Security of processing	(Clause 8.5) For the parties • To implement appropriate technical and organisational measures to ensure the security of the personal data, taking account of the relevant factors affecting the security assessment. In tackling data breach incidents, For data importer • To take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects. If the personal data breach in question is likely to result in a risk to the rights and freedoms of natural persons, For data importer • To notify without undue delay both the data exporter	(Clause 8.6) For the parties To implement appropriate technical and organisational measures to ensure the security of the personal data, taking account of the relevant factors affecting the security assessment. In tackling data breach incidents, For data importer • To take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects. • To notify without undue delay the data exporter (and the controller, where appropriate): (i) the details of a contact point; (ii) categories and approximate number of data subjects and personal data records concerned; (iii) its likely consequences; and (iv) the measures taken or proposed to address the breach. • To cooperate with the data exporter in notifying the competent supervisory authority and the affected data subjects (or in notifying the controller which may in turn notify the competent supervisory authority and the affected data subjects, as the case may be).	(Clause 8.2) For the parties • To implement appropriate technical and organisational measures to ensure the security of the personal data, taking account of the relevant factors affecting the security assessment. In tackling data breach incidents, For data exporter • To notify the data importer without undue delay the personal data breach. • To assist the data importer in addressing the breach.

	and the competent supervisory authority: (i) categories and approximate number of data subjects and personal data records concerned; (ii) its likely consequences; (iii) the measures taken or proposed to address the breach; and (iv) the details of a contact point. • To notify without undue delay the data subjects concerned of the personal data breach and its nature: (i) its likely consequences; (ii) the measures taken or proposed to address the breach; and (iii) the details of a contact point. The requirement of notifying data subjects concerned may not be applicable when the data importer has implemented measures to significantly reduce the associated risks or a notification would involve disproportionate efforts. In the latter case, a public communication may be adopted to inform the public of the personal data breach.		
Transfer of sensitive data	(Clause 8.6 or 8.7, as the case may be)		N/A

	For data importer • To apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the potential risk(s) involved.			
Onward transfers	(Clause 8.7) For data importer Not to disclose the personal data to a third party located outside the EU/EEA unless • the third party is or agrees to be bound by the appropriate module of the New SCCs; or • under the specified circumstances (e.g., it is necessary in order to protect the vital interests of the data subject or of another natural person, etc.).	(Clause 8.8) For data importer To disclose the personal data to a third party only • on documented instructions from the data exporter or the controller (as the case may be); or • if the third party (located outside the EU/EEA) is or agrees to be bound by the appropriate module of the New SCCs; or • under the specified circumstances (e.g., it is necessary in order to protect the vital interests of the data subject or of another natural person, etc.).		N/A
Processing under the authority of the data importer	(Clause 8.8) For data importer • To ensure that any person acting under its authority, including the data processor, processes the data only on its instructions.	N/A	N/A	N/A
Documentation and compliance	(Clause 8.9) For data importer • To keep appropriate documentation of its processing activities and make the same available to the competent supervisory	(Clause 8.9) For data importer • To deal with enquiries from the data exporter. • To keep appropriate documentation of its processing activities. • To allow for and contribute to	(Clause 8.9) For data importer • To deal with enquiries from the data exporter or controller. • To keep appropriate documentation of its processing activities.	(Clause 8.3) For data exporter • To make available to the data importer all information necessary to demonstrate compliance with the New SCCs.

	authority on request.	audits of the processing activities, at the request of the data exporter. For the parties • To make the documentation and relevant information available to the competent supervisory authority on request.	• To allow for and contribute to audits of the processing activities by the data exporter. For data exporter • To make the results available to the controller. For the parties • To make the documentation and relevant information available to the competent supervisory authority on request.	• To allow for and contribute to audits.

Q14. Is a data importer allowed to sub-contract any of its processing activities performed on behalf of the data exporter under the New SCCs to a sub-processor?

A: *From a controller to a processor; From a processor to another processor*

The relevant clause for engagement of sub-processors is Clause 9 of the New SCCs.

A data importer in the capacity of a processor may further engage a sub-processor with the specific prior authorisation or general written authorisation given by the data exporter (or the controller in the case of transfer from a processor to another processor).

The data importer is required to engage the sub-processor by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under the New SCCs (including third-party beneficiary rights for data subjects). It shall also provide for a third-party beneficiary clause under which the data exporter shall have the right to terminate the sub-processor contract and instruct the sub-processor to erase or return the personal data in question, in the event that the data importer has factually disappeared, ceased to exist in law or has become insolvent.

The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's contractual obligations.

Disclaimer

The information provided in this publication is for general reference only. It does not serve as an exhaustive guide to the application of the New SCCs and does not constitute legal or other professional advice. The Privacy Commissioner for Personal Data makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this publication. Organisations and individuals who want to adopt the New SCCs should seek professional legal advice.

First published in September 2021
Office of the Privacy Commissioner for Personal Data, Hong Kong