THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS

OVERVIEW

INTRODUCTION

On 4 June 2021, the European Commission adopted **two sets of standard contractual clauses**, one for the use between controllers and processors within the European Economic Area[1] (EEA) and one for the transfer of personal data to countries outside of the EEA. The purpose of these Q&As is to provide **practical guidance on the use of the SCCs** to assist stakeholders with their compliance efforts. The information in this document does **not constitute legal advice**. Instead, it is provided for general informational purposes only. The monitoring and enforcement of compliance with EU data protection law by controllers and processors falls within the competence of the national supervisory authorities and courts. The list and contact details of national data protection authorities in the EEA is available here: https://edpb.europa.eu/about-edpb/about-edpb/members_en.

These Q&As are based on **feedback received from various stakeholders** on their experience with using the new SCCs in the first months after their adoption. This page is intended to be **a 'dynamic' source of information** and its content will be updated as new questions arise.

I. STANDARD CONTRACTUAL CLAUSES

GENERAL

1. What are Standard Contractual Clauses?

Standard contractual clauses (SCCs) are **standardised** and **pre-approved model data protection clauses** that allow controllers and processors to comply with their obligations under EU data protection law. They can be incorporated by controllers and processors into their contractual arrangements with other parties, for instance commercial partners. There is **no obligation** to use SCCs. The clauses **can be used on a voluntary basis** to demonstrate compliance with data protection requirements, in which case they require a binding contractual commitment to abide by them. The European Commission has the power to adopt SCCs (1) for the relationship between controllers and processors and (2) for the transfer of personal data to countries outside of the EEA.

2. Which Standard Contractual Clauses have been adopted by the European Commission?

On 4 June 2021, the Commission adopted **two sets of Standard Contractual Clauses** (SCCs).

(1) **SCCs for the relationship between controllers and processors** fulfil the requirements in Article 28(3) and (4) of Regulation (EU) 2016/679 (the General Data Protection Regulation, 'GDPR') and in Article 29(3) and (4) of Regulation (EU) 2018/1725 (the Data Protection Regulation applicable to EU institutions, bodies, offices and agencies, 'EUDPR'). Consequently, these SCCs can be used by public and private entities as well as by EU institutions, bodies, offices and agencies. The SCCs thereby provide a coherent approach for the relationship between controllers and processors throughout the EEA. The SCCs are available here: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors

(2) **SCCs as a tool for data transfers**, i.e. to comply with the requirements of the GDPR for **transferring personal data to countries outside of the EEA**. They contain specific data protection safeguards to ensure that personal data continues to benefit from a high level of protection when

[1] The EEA is comprised of the 27 Member States of the EU as well as Iceland, Liechtenstein and Norway.

transferred outside the EEA. They can be used by data exporters, **without the need to obtain a prior authorisation** (for the data transfer or the clauses used) from a data protection authority. By adhering to the SCCs, data importers contractually commit to abide by a set of data protection safeguards. The SCCs are available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

3. What are the advantages of using SCCs?

Through their standardisation and pre-approval, SCCs are a **"ready-made"** and easy-to-implement tool. This is particularly important for SMEs or other companies that may not have the resources to negotiate individual contracts with each of their commercial partners. It also distinguishes the SCCs from other compliance mechanisms that require prior authorisation by a national data protection authority (e.g. ad hoc contracts for data transfers) or are typically more costly to implement (e.g. certification schemes).

As regards the **SCCs for data transfers**, feedback from stakeholders shows that they are by far the **most used data transfer instrument** for European companies. For example, according to the IAPP-EY Annual Privacy Governance Report 2019, "the most popular of these [transfer] tools – year over year – are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers […]".

4. What was the process followed by the European Commission in developing the SCCs?

In preparing the two sets of SCCs, the Commission sought **stakeholder input** to better understand the realities and needs on the ground and learn from their practical experience with using existing SCCs. The Commission received detailed feedback from various stakeholders (including industry, civil society, legal professionals and academics) through the GDPR Multi-Stakeholder Expert Group[2], a broad public consultation[3], dedicated workshops/roundtables and an independent external study.

5. Will the European Commission evaluate after some time how the new SCCs work in practice?

Article 97 of the GDPR requires the Commission to **perform a review of the GDPR's implementation every four years** (the 2020 evaluation report is available here https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en). **The next review is expected by 2024** and will also include an evaluation of the practical application of the SCCs.

[2] For more information, see https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3537.

[3] 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-_en and https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-&-processors-located-in-the-EU-implementing-act-_en.

SIGNATURE, MODIFICATIONS AND RELATIONSHIP WITH OTHER CONTRACTUAL PROVISIONS

6. Are there specific requirements for the signature of the SCCs by the parties?

The use of the SCCs to fulfil the requirements of the GDPR and EUDPR for the controller-processor relationship, or as a transfer tool, requires that the parties enter into a legally binding agreement to abide by them. To this end, the parties need to fill in the annexes to the SCCs and sign Annex I, which form an integral part of the clauses. Inter alia, the **parties have to provide** their contact details and information on their respective roles (who acts as controller and processor, or data exporter and data importer) under the clauses. The SCCs do not contain any requirements on how the signature should be formalised (e.g., whether it can be done electronically). This is left to **national (civil/contract) law governing the agreement**.

7. Can the text of the SCCs be changed?

The text of the SCCs may not be altered, **except** (i) to **select modules and/or specific options offered in the text**, (ii) to **complete the text** were necessary (indicated by square brackets), e.g. to indicate the competent courts and supervisory authority, and to specify time periods, (iii) to **fill in the Annexes** or (iv) to add **additional safeguards** that increase the level of protection for the data. These adaptations are not considered as altering the core text.

Specific information on the SCCs for controllers and processors: if the parties change the text of the SCCs themselves (beyond the adaptations mentioned below) they cannot rely on the legal certainty offered by an EU act.

Throughout the text, the parties need to make necessary adaptations by choosing one of the two options provided for in the SCCs concerning:

- Compliance with the GDPR or compliance with the EUDPR;
- Prior specific authorisation or general written authorisation given by the controller to the processor for engaging sub-processor(s).

Specific information on SCCs for data transfers: if the parties change the text of the SCCs themselves (i.e. beyond choosing the relevant modules and/or options and filling in square brackets and annexes), the modified clauses may no longer be used as a basis for data transfers to third countries, unless they are approved by a national data protection authority as "ad hoc clauses" (pursuant to Article 46(3)(a) of the GDPR).

8. Is it possible to add additional clauses to the SCCs or incorporate the SCCs into a broader commercial contract?

The parties may **supplement** the SCCs with additional clauses or **incorporate** them into a broader commercial contract, **as long as** the other contractual provisions **do not contradict the SCCs**, either directly or indirectly, or prejudice the rights of data subjects.

Example: where the SCCs require the parties to inform each other or cooperate, the parties may agree on additional clauses that lay down how the communication/cooperation between the parties will take place in practice.

Example: the SCCs require the data importer to notify the data exporter about a data breach without undue delay after having become aware of it. The parties may specify the time frame in which this notification has to be provided, without undermining the general approach (e.g. without undue delay, and in any event no later than 72 hours after the data importer becomes aware of the breach).

Example: Clause 12(a) of the SCCs international data transfers specifically regulates the liability between the parties. The parties may not include a general exculpation from liability (i.e. covering also the clauses of the contract that incorporate the SCCs) in the commercial contract, as this would contradict this provision of the SCCs. In addition, it would likely prejudice the rights and freedoms of individuals, e.g. by reducing the incentive for the parties to ensure compliance with the SCCs.

Example: Clause 7.7 of the SCCs for controllers and processors imposes an obligation on the processor to request an authorisation from the controller when it engages a sub-processor. The parties may not include in a broader commercial contract between the controller and the processor a clause, which allows the processor to sub-contract data processing without such obligation to consult and request an authorisation from the controller as this clause will directly contradict clause 7.7 of the SCCs.

9. Can the parties delete modules and/or options that do not apply to their situation?

When relying on SCCs, the parties should only agree the clauses that are relevant for their situation. The modules and/or options that do not apply should be deleted.

Example: a controller wants to transfer personal data to another controller relying on the SCCs for international data transfers. All general clauses for which no modules are indicated (e.g. Section I) and the clauses that are relevant for Module 1 from the SCCs should be extracted. All clauses that relate only to other modules may be deleted.

Example: in Clause 7.7 of the SCCs between controllers and processors (use of sub-processors), the parties have to choose one of the two options for authorising the hiring of sub-processors by the data importer. If they choose Option 1, Option 2 should be deleted from the SCCs.

Example: a company based in the EEA acting as a controller wants to establish a contractual relationship with a processor in the EEA. To comply with Article 28(3) and (4) of the GDPR, it may use the SCCs for the relationship between controllers and processors. In this case, it has to choose OPTION 1 (which refers to the GDPR) throughout the text of the SCCs and delete the references to OPTION 2 (which concerns compliance with the EUDPR).

10. How should the SCCs be incorporated into a commercial contract?

To be able to rely on the SCCs and ensure transparency, they **have to be signed by and binding** on all parties, and **incorporated into their contract**, in accordance with civil law requirements from the chosen jurisdiction. In addition, the SCCs should be applied to the situation of the parties (e.g. to the covered data transfers), by **filling in the annexes** and making clear (to the parties, as well as to the concerned data subjects, competent data protection authorities and courts) **which modules, options and specifications (between square brackets) have been chosen**.

CHANGES TO THE PARTIES

11. What is the purpose of the so-called 'docking clause'?

The docking clause is an **optional clause** by which the parties to the SCCs can choose to agree that **additional parties may join** the contract in the future. This provides the parties with additional flexibility in case of changes with respect to the entities participating in the processing arrangement throughout the life cycle of the contract (e.g. in case it becomes necessary to extend the processing chain by including a further (sub-)processor).

Example: a processor offers the same services to several controllers. A few years after having concluded SCCs to comply with Article 28 of the GDPR with one controller, both parties agree that a second controller can join the contract by making use of the docking clause.

Example: a controller transfers personal data to a processor in a third country based on the SCCs for international transfers (using Module 2). When the processor wants to hire a sub-processor, the parties agree that the sub-processor can adhere to the initially concluded SCCs (using Module 3).

12. How does the docking clause work in practice? Are there any formal requirements for allowing new parties to accede?

One or several new parties may adhere to the SCCs with the **consent of all the pre-existing parties**. The **formalisation** of such consent is not regulated by the SCCs, but should be done in accordance with relevant provisions of the **national law** governing the SCCs. For example, if allowed under applicable contract law, one party may be appointed by the others to agree to the accession of a new party on behalf of all pre-existing parties. Once this authorisation is formalised, the new party will need to complete the Annexes and **sign Annex I of the SCCs** in order to make such accession effective. Amending the main agreement to which the SCCs are annexed, by adding parties to that agreement, is not sufficient to add parties to the SCCs.

13. What happens when a new party accedes to the SCCs? Are there any formalities to take care of?

Upon accession to the SCCs, the new party assumes **all the rights and obligations according to its role** (e.g. data exporter or importer, controller or processor). The **other parties simultaneously have the relevant rights and obligations vis-à-vis the new party** (e.g. any obligation to provide assistance in answering data subject requests, etc.).

The **Annexes to the SCCs** must be **updated** when parties are added. For example, when new parties accede, these parties and their roles should be listed and, where relevant, the description of the transfers and applicable technical and organisational measures brought up to date accordingly.

II. STANDARD CONTRACTUAL CLAUSES BETWEEN CONTROLLERS AND PROCESSORS

14. What is the difference between SCCs adopted by national data protection authorities and the SCCs adopted by the Commission?

Article 28(8) of the GDPR empowers **national data protection authorities** to adopt SCCs for the relationship between controllers and processors. If a data protection authority adopts such SCCs, they apply only within the territory where that authority exercises its powers. Whether other data protection authorities will accept reliance on these SCCs depends on the individual decisions of those authorities.

Conversely, SCCs adopted by the **Commission** pursuant to Article 28(7) of the GDPR can be relied upon throughout the whole EEA and are binding on all EEA data protection authorities. The validity of the SCCs adopted by the Commission can be contested only before the Court of Justice of the European Union. They provide for a harmonised approach across the EEA and the legal certainty of an EU act.

15. In which form should instructions by the controller be given to the processor?

According to Clause 7.1 "The processor shall process personal data only on documented instructions from the controller". The SCCs **do not specify** in which form the instructions shall be given, therefore the controller can decide to provide those instructions in whatever form that is deemed appropriate (e.g. in writing or orally, through online tools and technical signals), but **on the condition that the instructions are documented**.

16. Is the processor required to provide the name(s) of the sub-processor(s) it engages to the controller?

Yes. Under clause 7.7 'Use of sub-processors' the **parties have to choose one of two options**: OPTION 1: PRIOR SPECIFIC AUTHORISATION or OPTION 2: GENERAL WRITTEN AUTHORISATION. **In both cases, the processor has to provide the name(s) of the individual sub-processor(s)** to the controller so that the latter is enabled to decide on the authorisation of the selected sub-processor(s). It is not sufficient for the processor to provide only the categories for the sub-processors. It is **for the parties to agree on the time period** for the processor to submit the request for prior specific authorisation (OPTION 1), or to inform in writing the controller of any intended changes of the agreed list of sub-processors (OPTION 2).

17. What happens if the controller objects to changes of sub-processors, in case a general authorisation to the engagement of sub-processors was given?

According to OPTION 2 in clause 7.7 of the SCCs the processor has to specifically inform in writing the controller of any intended changes of the agreed list of sub-processors, respecting an agreed time period of notice. If the controller objects to the intended changes, the processor may not engage the new sub-processor(s).

18. What is the required time period for the processor to notify the controller of a data breach?

The SCCs do not specify the time period for the processor to notify the controller of a data breach concerning data processed by the processor. Clause 9.2 of the SCCs indicates that this has to be

done “without undue delay”. It is therefore for the parties to determine this period taking into consideration the particular circumstances of the data processing at stake.

19. <u>Besides a review or an audit, can the processor demonstrate compliance with its requirements under the SCCs by other means?</u>

Yes. The processor can use adherence to an **approved code of conduct** pursuant to Article 40 of the GDPR or an **approved certification mechanism** pursuant to Article 42 of the GDPR to demonstrate to the controller that it complies with its obligations that are set out in the SCCs and stem directly from the GDPR. At the same time, this does not affect the possibility of the controller to decide on a review or an audit of the processing activities covered by these SCCs.

III. STANDARD CONTRACTUAL CLAUSES FOR DATA TRANSFERS TO THIRD COUNTRIES

REASONS FOR MODERNISATION AND MAIN NOVELTIES

20. Why did the Commission modernise the previous SCCs for international data transfers?

Under the previous **Data Protection Directive** (Directive 95/46/EC), the Commission adopted **three sets of SCCs:** two for transfers from an EEA-controller to a non-EEA controller (Commission Decisions 2001/497/EC and 2004/915/EC) and one for transfers from an EEA-controller to a non-EEA-processor (Commission Decision 2010/87/EU). These SCCs remained available after the GDPR entered into force. However, there was a **need to bring them in line with the new legal framework,** in particular to update them in light of new requirements of the GDPR and to take into account evolving case law of the EU Court of Justice (e.g. the so-called *Schrems II* judgment in Case C-311/18).

Moreover, t**he previous SCCs were no longer adapted to the realities of the modern digital economy**, with its diverse processing realities and long and often complex processing chains with multiple parties and sometimes changing roles. There was therefore a need to **modernise the "architecture"** of the SCCs, to make them more user-friendly, cover additional transfer scenarios (such as transfers from a processor to a (sub)processor) and provide additional flexibility, by allowing the accession of parties throughout the contract's lifecycle.

21. What are the main novelties compared to the previous SCCs?

The **core elements** that were already included in the SCCs adopted under the previous Data Protection Directive **have been maintained** in the modernised clauses. For example, like the former ones, the modernised SCCs contain commitments with respect to essential data protection principles, security obligations, third party beneficiary rights and submission to the jurisdiction of EEA data protection authorities and courts. At the same time, **important changes** have been introduced.

First, the **'architecture'** of the SCCs has been updated, for example:

- The SCCs cover **additional transfer scenarios**: whereas the scope of application of the previous SCCs was limited to data transfers from controllers to controllers and from controllers to processors, the modernised ones can be used in all of the most relevant cases: Controller to Controller (Module 1), Controller to Processor (Module 2), Processor to Processor (Module 3), and Processor to Controller (Module 4).
- Three separate sets of SCCs covering two transfer scenarios have been replaced by **one set of SCCs with a modular structure** (covering four transfer scenarios). The parties have to combine general clauses (that are applicable regardless of the specific transfer scenario) with the module(s) that applies to their situation.
- A **docking clause** now permits new parties to join the SCCs throughout the lifecycle of the contract.
- The SCCs are complemented by **annexes** where concrete information on the specific transfers must be provided, for example a list of the parties and their respective roles, a description of the

purposes of each individual transfer to take place under the agreement, a list of the security measures in place, the safeguards applied to protect sensitive data, etc.

Second, a number of **substantive changes** have been introduced, for example:

- The SCCs reflect **new requirements of the GDPR**, including enhanced transparency obligations and more detailed clauses on data subject rights, data breach notification and rules for onward transfers.
- For data transfers from controllers to processors, or processors to sub-processors, the **requirements of Article 28 of the GDPR** have been incorporated into the SCCs. Companies therefore do not need to sign a separate contract to comply with Article 28 of the GDPR.
- Clauses implementing the *Schrems II* judgment of the EU Court of Justice: the parties to the SCCs must now carry out a **"transfer impact assessment"** documenting the specific circumstances of their transfer, the laws in the country of destination and the additional safeguards they put in place to protect the personal data.
- **New obligations in case of access by public authorities to the data transferred**, e.g. the obligation to provide information to data exporters and to challenge unlawful requests.

22. Are data exporters and importers that still use the "old" SCCs (adopted under the 1995 Data Protection Directive) required to switch to the new ones (adopted in 2021)?

Agreements to transfer data concluded **after 27 September 2021** must be based on the **new SCCs.**

For those entities that **entered into a transfer agreement based on the previous SCCs before 27 September 2021,** a transition period is granted **until 27 December 2022 to switch to the new SCCs** (i.e. replace the previous with the new SCCs, including the annexes)**.** However, organisations have to switch to the new SCCs already before that date if the data processing operations that are governed by the contract are modified.

Example: a data exporter and importer have concluded a service agreement before 27 September 2021, relying on the previous SCCs for their data transfers. In February 2022, there is a change in the prices set out in the service agreement. As this does not affect the processing of personal data under the SCCs, this change does not require the parties to switch to the new SCCs (although they will still have to do so by 27 December 2022).

Example: a data exporter and importer have concluded a service agreement before 27 September 2021, relying on the previous SCCs for their data transfers. In February 2022, the parties agree that additional categories of data will be transferred. This change affects the processing of personal data under the SCCs and the parties therefore need to switch to the new SCCs.

After 27 December 2022, it will **no longer be possible to rely** on the previous SCCs to lawfully transfer personal data to third countries.

SCOPE OF APPLICATION AND TRANSFER SCENARIOS

23. For which transfers can the SCCs be used?

The SCCs can be used by controllers or processors that are subject to the GDPR to transfer personal data to controllers or processors outside the EEA whose activities are not subject to the GDPR.

First, the SCCs can be used by **controllers and processors in the EEA to transfer data outside the EEA**, in particular:

- By an EEA controller, to transfer personal data to a controller or processor outside the EEA that is not subject to the GDPR;
- By an EEA processor, to transfer personal data to a sub-processor or to a controller outside the EEA (on whose behalf it is processing the data) that is not subject to the GDPR.

Example: a Czech company uses the SCCs to transfer data of its employees to a payroll provider in Singapore.

Second, **the direct applicability of the EU data protection rules extends to certain processing operations of controllers and processors outside the EEA**, for example because they specifically target the EEA market by offering goods or services to individuals (for more information and guidance, see the guidance of the European Data Protection Board, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf). The SCCs can therefore also be used by those **non-EEA controllers and processors for data transfers related to these processing operations to non-EEA entities**, in particular:

- By a controller outside the EEA whose processing is subject to the GDPR to a controller or processor outside the EEA that is not subject to the GDPR;
- By a processor outside the EEA whose processing is subject to the GDPR to a sub-processor or to a controller outside the EEA (on whose behalf it is processing the data) that is not subject to the GDPR.

Example: a travel agency in Thailand is directly subject to the GDPR pursuant to its Article 3(2), because it offers tourist travel packages targeted at European customers (as the offer of these packages is made in languages used in the EEA, is adapted to the needs and preferences of European tourists, with the possibility to pay in Euro or another currency used in the EEA, etc.). To arrange accommodation in Thailand, the agency has an ongoing arrangement with a local hotel. The travel agency may use the SCCs (Module 1) to share the personal data of European tourists with the hotel.

24. Can these SCCs be used for data transfers to controllers or processors whose processing operations are directly subject to the GDPR?

No (see Article 1 of Decision (EU) 2021/914[4]). These SCCs provide a comprehensive data protection framework that has been developed to ensure continuity of protection in case of data transfers to data importers that are not subject to the GDPR. They do not work for importers whose processing

[4] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

operations are subject to the GDPR pursuant to Article 3, as they would duplicate and, in part, deviate from the obligations that already follow directly from the GDPR. The **European Commission is in the process of developing an additional set of SCCs for this scenario**, which will take into account the requirements that already apply directly to those controllers and processors under the GDPR.

25. Can the SCCs be used to transfer personal data to an international organisation?

The SCCs are designed for a commercial context and are **not adapted for data transfers to international organisations**. For example, international organisations that benefit from specific privileges and immunities (e.g. following from international or headquarter agreements) may not be able to accept the jurisdiction of an EEA data protection authority or court. Other instruments that take into account the status of such international organisations should therefore be used for such transfers, e.g. tailor-made contracts or administrative arrangements approved by the data protection authorities. In addition, the European Commission is in the process of developing SCCs that could be used by service providers to transfer data to international organisations.

26. Can the SCCs only be used for international data transfers under the GDPR?

Several **other jurisdictions** have **endorsed the EEA SCCs** as a transfer mechanism under their own national data protection legislation, with limited formal adaptations to their domestic legal order (e.g. the United Kingdom[5] and Switzerland[6]). This can significantly facilitate compliance with applicable rules for companies active both in the EEA and these jurisdictions.

Others have developed **model clauses that share a number of commonalities** with the EEA SCCs. This includes clauses developed at national level (e.g. New Zealand[7], Argentina[8]) and within the framework of regional organisations (e.g. the clauses adopted by the Ibero-American Data Protection Network[9] and the Association of Southeast Asian Nations[10]). Work on modernised model clauses for cross-border transfers is also ongoing in the Consultative Committee of Council of Europe Convention 108.

27. What are the different 'modules' and how should the right one be chosen?

The SCCs combine **general clauses** applicable in all cases (e.g. Section I) with **four modules** that are adapted to different transfer scenarios. The **parties have to choose the module that corresponds to their situation**, in particular in light of their different roles, i.e. whether they are controllers, processors or sub-processors (regarding the meaning of these concepts, see also the guidance of the European Data Protection Board, available here https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en), and who acts as data exporter and importer:

---

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.
[6] https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html.
[7] See https://privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/.
[8] See http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm.
[9] See https://www.redipd.org/sites/default/files/2021-11/red-iberoamericana-clausulas-contractuales-2021.pdf.
[10] See https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

Module 1 applies to data transfers from a **controller** (the data exporter) to another **controller** (the data importer).

Example: a Swedish travel agency has a framework contract with a hotel chain to arrange accommodation for European tourists around the world. To transfer data of the guests to the chain's booking centre (the data importer) based on the SCCs, the Swedish agency (the data exporter) should use Module 1.

Module 2 applies to data transfers from a **controller** (the data exporter) to a **processor** (the data importer).

Example: a company in the Netherlands outsources its HR services to a provider in India. The Dutch company (the data exporter) should use Module 2 to transfer the data of its employees to the Indian provider (the data importer) based on the SCCs.

Module 3 applies to data transfers from a **processor** (the data exporter) to a **sub-processor** (the data importer).

Example: a hospital in Germany shares blood samples with a laboratory in Poland for analysis. The Polish laboratory outsources some aspects of its work to an Indonesian institute specialising in genetic analysis, using the SCCs. The Polish laboratory (the data exporter) may use Module 3 to transfer the data to the Indonesian institute (the data importer).

Module 4 applies to data transfers from a **processor** (the data exporter) to its **controller** (the data importer).

Example 1: a Moroccan company uses cloud services offered by a Luxembourg company to manage its customer database. The SCCs (Module 4) can be used by the Luxembourg company (the data exporter) to transfer the data from its server in Luxembourg (back) to the Morocco client (the data importer).

Example 2: a university in Tunisia hires a research institute in Belgium to carry out a survey for which it collects and processes data in the EU and sends it to the university. The SCCs (Module 4) can be used by the Belgian institute (the data exporter) to transfer the data to the university in Tunisia (the data importer).

28. Can several modules be agreed between the same parties at the same time?

Yes. As explained in the reply to Q26, the parties have to choose the module(s) that correspond to their situation. It **may occur that the parties assume different roles** for different data transfers taking place between them as part of their overall contractual relationship. If this is the case, they **should use the appropriate module** for each such transfer. For example, for some data transfers by a controller (data exporter), the data importer may act as a controller, whereas it may be a processor for others. In that case, the parties may use both Module 1 (for those transfers for which both the data exporter and data importer act as controllers) and Module 2 (for those transfers for which the data exporter acts as controller and the data importer as processor).

29. How can compliance with Article 28 of the GDPR be ensured when transferring data to a processor or a sub-processor outside of the EEA?

The **requirements of Article 28 of the GDPR have been incorporated** into Module 2 (controller-to-processor transfers) and 3 (processor-to-processor transfers) of the SCCs. By using these modules,

controllers and processors do not need to enter into a separate data processing agreement, as they can ensure compliance both with the requirements of Article 28 of the GDPR and the requirements for international data transfers (Article 46 of the GDPR).

There may also be situations where SCCs for data transfers are not needed because another instrument is available, e.g. if the processor or sub-processor is located in a country that benefits from an adequacy decision. In that case, the data exporter can use the SCCs for the relationship between controllers and processors to ensure compliance with Article 28 of the GDPR.

30. In which scenarios should Module 4 (processor to controller) be used?

Module 4 should be used where a **processor in the EEA** is hired by a **controller outside the EEA**, either to collect data in the EEA on behalf of the controller or to process data received from the controller in the EEA. In those cases, the SCCs can be used by the processor to transfer the data (back) to its controller.

Example: a Moroccan company uses cloud services offered by a Luxembourg company to store data on its customer database. The SCCs (Module 4) can be used to transfer the data from Luxembourg (by the data exporter) (back) to Morocco (to the data importer).

Example: a Chilean company instructs a Spanish service provider to conduct market research and develop marketing material, using client data received from the Chilean headquarters and client data it has collected in Spain. Module 4 of the SCCs can be used by the Spanish provider to transfer aggregated data on the two data sets to Chile.

INDIVIDUALS: YOUR RIGHTS WHEN YOUR DATA IS TRANSFERRED BASED ON THE SCCs

31. How can I know that my data is transferred outside of Europe based on the SCCs?

Information about the transfer of your data outside of the EEA **should be provided by the data exporter** that is processing your data: Articles 13 and 14 of the GDPR require data exporters to inform you, among others, about their intention to transfer personal data outside of the EEA. **If they are using SCCs**, they **should also inform you thereof and explain how you can obtain a copy** of the clauses.

If SCCs are used, **a data importer outside of Europe may also have to provide you with certain information** (e.g. its contact details, the categories of personal data it processes and recipients with whom your data may be shared), see Module 1, Clause 8.2(a) of the SCCs. This will be the case if the importer will use the data it receives for its own purposes (i.e. different purposes than the ones for which the data was processed by the data exporter).

32. I have been informed that my data has been transferred outside the EEA based on SCCs. How can I obtain more information about the actual transfers, my rights as a data subject and the applicable safeguards? Can I obtain a copy of the SCCs?

The SCCs require the parties to provide you, on request and **free of charge**, with a **copy** of the clauses, **as they have been used**. This includes the modules/options as selected, as well as the completed and signed annexes (where the parties have to provide details about the data transfer and certain measures taken to protect them during processing by the data importer). A **general**

reference to the SCCs as adopted by the European Commission (e.g. by providing a link to the Commission's website) **is not sufficient** (see Module 1, Clause 8.2 of the SCCs; Module 2, Clause 8.3 and Module 4, Clause 8.3). When providing you with a copy of the clauses, the parties **may only redact information** that concerns business secrets or other confidential information (e.g. personal data of other individuals), but have to explain why it was left out. If the remaining text becomes too difficult to understand, the parties must provide a meaningful summary of the redacted parts (see Module 1, Clause 8.2 of the SCCs; Module 2, Clause 8.3 and Module 4, Clause 8.3).

In addition, under the GDPR and the SCCs, you have the **right to obtain information** (e.g. on the data that is transferred, the purpose of the processing, the recipients with whom your data has been or will be shared, and the right to lodge a complaint with a supervisory authority) **from the entity that is responsible for the processing of your data** (i.e. the 'controller'). In particular, you can request information about the handling of your data, including data transfers, from a data exporter acting as a controller pursuant to Article 15 of the GDPR. If data has been transferred by a controller to an entity outside the EEA that uses your data for its own purposes (i.e. as another 'controller'), the data exporter will only be able to provide information about its own activities (in addition to the fact that data is transferred outside the EEA). However, in that case, you can exercise your right to obtain information directly against the controller outside the EEA based on the SCCs (Module 1, Clause 10 of the SCCs).

If several entities are involved in the processing of your data and you do not know who the controller is, you can either contact (1) the **entity that has transferred your data** (the data exporter) or (2) the **entity outside of Europe that has received your data** (the data importer). If the entity you turned to is not able to respond to you directly (because it only acts as a service provider on behalf of the other entity), the SCCs require both parties to cooperate to handle your request in an effective and timely manner.

33. What if my data was processed in violation of the SCCs, can I obtain redress (e.g. compensation for damages)? Where can I lodge a complaint?

The **SCCs provide different avenues to obtain redress**, both against the data exporter and the data importer. In particular, even though you are not a party to the SCCs, the SCCs allow you **to enforce those clauses that** contain specific safeguards for the use of your data **directly against the parties** as a third party beneficiary (see Clause 3 of the SCCs).

First, you have the possibility to lodge a **complaint directly with the data importer**, who should have designated a specific contact point to handle complaints (see Clause 11(a) of the SCCs). If the data importer offers the possibility to lodge a complaint with an **independent dispute resolution body**, you can also turn to that body.

Second, you have the possibility to lodge a complaint before the **data protection authority of the EEA country where you are a resident.** You can bring such a complaint directly against the data importer, if you consider that it has acted in violation of the SCCs (see Clause 11(c) of the SCCs) or against the data exporter, if you consider that it has processed your data unlawfully (see Article 77 of the GDPR).

Third, you can **initiate proceedings in court** against the parties to the SCCs, for instance to obtain injunctive relief or claim compensation for damages. In particular, the parties to the SCCs are liable for any material or non-material damages that they cause you by breaching the provisions of the SCCs that that provide safeguards for the handling of your data or ensure specific rights (see Clause

12 of the SCCs). Such actions can be brought before the competent court of the EEA country (as determined by national law) in which you live or the courts in the EEA that have been designated by the parties to the SCCs (see Clause 18(b) and (c) of the SCCs).

Special rules apply if your data has been transferred by **a service provider in the EEA that acts on behalf a non-EEA entity**. In this case, you have the possibility to lodge a complaint directly with the data importer (i.e. the controller outside of the EEA) or, if available, an independent dispute resolution body (see Module 4, Clause 11). You can also turn to the data exporter in the EEA, who will have to cooperate with the data importer to handle your request (see Module 4, Clause 10). In addition, you can **initiate proceedings in court** against the parties to obtain injunctive relief or claim compensation for damages (see Module 4, Clause 18, together with Clause 3). Such actions can be brought before the courts that have been designated by the parties to the SCCs.

Finally, it is important to note that the abovementioned possibilities to obtain redress only concern those that are available under the SCCs themselves. **This does not affect the possibility for individuals to obtain redress against the data exporter based on the GDPR**. In particular, individuals always have the right to lodge a complaint with a national data protection authority (Article 77 of the GDPR) and to obtain a judicial remedy (Article 79 of the GDPR) concerning the handling of their data by the data exporter.

OBLIGATIONS OF DATA EXPORTERS AND IMPORTERS

34. For Modules 1, 2 and 3: does the data importer have to take specific steps when sharing personal data it has received with third parties?

As a general rule, when sharing data received under the SCCs with another entity inside or outside its country of establishment, the data importer has to ensure that it **continues to benefit from similar protections** (see Module 1, Clause 8.7; Module 2, Clause 8.8 and Module 3, Clause 8.8). This can be done in different ways, for example if the **third party accedes to the SCCs** or by concluding a **separate contract with the third party ensuring similar protections** to those provided under the SCCs.

The data importer may also further share the data in **certain specific situations**, where it is not possible or not appropriate to agree on (contractual) data protection safeguards with the third party recipient. In particular, it may be necessary for the importer to share information **to protect the vital interests of an individual**, e.g. a hotel chain having to disclose data of a guest to a local hospital in the context of a medical emergency. The same applies where the importer has to disclose certain information **as part of domestic administrative, regulatory or judicial proceedings**, e.g. a pharmaceutical company that needs to share data with a domestic regulatory authority in order to obtain approval of its products.

Additional information for Module 1 (controller to controller): if none of the above apply, the data importer may also rely on the explicit consent of concerned data subjects to further transfer the data to third parties (see Module 1, Clause 8.7(vi)). In this case, the importer has to make sure that the individual is informed about the purpose(s) of the transfer, the identity of the recipient and the possible risks to the individual posed by the transfer due to the lack of data protection safeguards. The data importer also has to inform the data exporter about onward transfers based on consent. The data exporter may request a copy of the information provided to the individual.

35. Can liability under the SCCs be limited by general liability clauses in the main services/commercial agreement?

The SCCs regulate two types of liability: (1) **liability of the parties towards data subjects** (see Module 1 and 4, Clause 12(b) and (c); and Module 2 and 3, Clause 12(b), (c) and (e) of the SCCs) and (2) **liability between the parties** (see Module 1 and 4, Clause 12(a); and Module 2 and 3, Clause 12(a) of the SCCs). **Other clauses** in the broader (commercial) contract (e.g. special rules on the distribution of liability, liability caps in the relationship between the parties) **may not contradict or undermine these liability schemes of the SCCs** (see also Clause 2(a) of the SCCs).

Conversely, it is important to note that **this only applies to liability for violations of the SCCs** themselves. The liability clauses of the SCCs **do not affect liability provisions that may apply to other aspects** of the contractual relationship between the parties.

36. What is the effect of the termination of the SCCs on other contractual arrangements between the parties?

Clause 16 entitles the data exporter to **temporarily suspend the transfer** of personal data to the data importer in the event the latter is in breach of the Clauses or is unable to comply with them. Moreover, in certain (particularly serious) cases the data exporter will be entitled to **terminate** "the contract, insofar as it concerns the processing of personal data under th[e] Clauses". This means that the right to termination under Clause 16 is **limited to the parts of the contract that concern the processing of personal data under the SCCs**.

As Clause 2(a) clarifies, parties are in principle allowed to include the SCCs in a wider (commercial) contract. The arrangements agreed to in this **wider contract** – as well as the law applicable to it – **will determine whether a breach of the Clauses will affect the wider contract**, in particular whether the data exporter will have a right to terminate the entire contractual relationship.

Where the processing operations governed by the SCCs involve **more than two parties**, the data exporter may exercise this **right to termination only with respect to the relevant Party**, unless the parties have agreed otherwise (see Clause 16(c)).

37. Are there any requirements for choosing the law applicable to the contract?

Clause 17 requires the parties to indicate the law that will govern the application of the SCCs ("governing law"). For **Module 1, 2 and 3**, this always has to be the **law of one of the EU Member States or EEA countries**. For **Module 4**, this may also be the **law of a non-EEA country**.

For all modules, this **must be a domestic legal regime** that allows for "**third party-beneficiary rights**" within the meaning of Clause 3. This means that the chosen law must allow private parties to create contractually rights that can be invoked by the individuals concerned, i.e. the data subjects whose personal data will be transferred based on the SCCs.

For Modules 2 and 3, the SCCs specifically provide that the governing law will in principle be the law of the EEA country in which the data exporter is established, unless this law does not allow for the creation of third party-beneficiary rights (in which case the parties must choose another law).

Clause 17 **should be read in combination with Clause 4**, which clarifies that the SCCs shall be read and interpreted in light of the provisions of the GDPR – in particular, where they use terms

specifically defined in the GDPR – and shall not be interpreted in a way that conflicts with rights and obligations provided therein. The governing law agreed according to Clause 17 will nevertheless be relevant, for instance when it comes to the determination of specific time limits.

38. For Module 1, 2 and 3: which data protection authority should be designated as the competent authority?

When entering into the SCCs, the **data importer** agrees to **submit itself to the jurisdiction** of an EEA data protection authority (Clause 13). This means that the data importer agrees to cooperate with that authority in any procedure that concerns compliance with the SCCs (e.g. investigations, inquiries and audits) and to abide by its decisions (e.g. orders to bring a processing activity in compliance with the SCCs).

The parties should designate the competent data protection authority in Annex I.C to the SCCs. If there is more than one data exporter, several supervisory authorities may be competent. Clause 13 of the SCCs indicates how to determine which authority will be competent.

If the data exporter is established in the EEA, the designated data protection authority should be the one that is competent to oversee compliance by the exporter with the GDPR. For businesses carrying out cross-border processing activities in the EEA, this will be the lead supervisory authority.

If the data exporter is not established in the EEA but is directly subject to the GDPR, the competent data protection authority will be:

- If the exporter has to appoint a representative (in accordance with Article 27 of the GDPR): the data protection authority of the EEA country where the representative is established;
- If the exporter does not have to appoint a representative (in accordance with Article 27 of the GDPR): the data protection authority of the/a EEA country where the data subjects whose data is transferred are located.

At the same time, it is important to note that the **SCCs also allow data subjects to lodge a complaint** with the data protection authority in the EEA country of **their habitual residence or place of work**. If this is a different authority than the one that has been designated by the parties, the two authorities will cooperate in handling the complaint.

39. Are there any requirements for filling in the annexes? How detailed should the information be?

The parties must clarify to **which specific data transfers** they intend to apply the SCCs, in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred (Annex I.A and B). Moreover, the parties need to clarify their **respective roles** (as "data exporter" or "data importer"), including in case of subsequent changes based on the (optional) docking clause (Clause 7), and, for data exporters located outside the EU but covered by the GDPR (Article 3(2)), indicate their representative in the EU designated pursuant to Article 27 of the GDPR. The parties also need to indicate the **competent supervisory authority/authorities**, in accordance with Clause 13 (Annex I.C, see question 38 for more information on choosing the competent authority).

In addition, while the SCCs set out general requirements with respect to **data security** and the **processing of sensitive data**, these requirements need to be further specified with respect to the

data transfer at issue (Annex I.B and Annex II). With respect to security, Annex II contains a list of examples of possible measures that can be put in place. The parties are not required to list each of these measures, but should describe those measures that are actually implemented by the data importer to ensure an appropriate level of security.

The **place to provide this specific information is the Appendix**, which according to Clause 1(d) forms an "integral part" of the SCCs. In filling out this Appendix, **the parties should carefully consider the "Explanatory Note"** on top of the first page of the Appendix and – specifically with respect to technical and organisational (security) measures – at the beginning of Annex II.

Examples of information to be provided in the annexes (see also the guidance of the European Data Protection Board, e.g. on transparency (available at https://ec.europa.eu/newsroom/article29/items/622227/en) and the controller-processor relationship (available at https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf):

- Categories of data subjects whose data is transferred: e.g. employees, customers (natural persons), persons who are members of a loyalty programme, natural persons who have subscribed to e-mails, children to whom information society services are offered, etc.
- Categories of personal data transferred: e.g. name, surname, e-mail address, telephone number, address of the place of residence, national identification number, detailed information on payments, information regarding health records, etc.
- Purposes of the transfer and further processing: detecting unlawful activity, payroll administration, carrying out bank payments, providing customer support, market research, etc.
- Nature of the processing: e.g. storage, recording, publication, combination, sorting, dissemination, etc.
- Period for which the data will be retained or the criteria used to determine that period: a specific period could for instance be determined by statutory requirements (e.g. X years). When it is not possible to provide an exact period, it must be explained how the retention period will be determined, e.g. on the basis of industry guidelines, the duration of the processing agreement etc. If different categories of personal data are subject to different retention periods, each period must be described separately.

LOCAL LAWS AND GOVERNMENT ACCESS

40. Are any specific steps needed to comply with the Schrems II judgment when using the new SCCs? Is it still necessary to take into account the guidance of the EDPB?

In line with the *Schrems II* judgment (C-311/18) of the EU Court of Justice, **Clause 14** requires the parties to assess, prior to concluding the SCCs, whether the laws and practices of the third country of destination applicable to the processing of the personal data by the data importer, could prevent the latter from complying with the Clauses. In carrying out this **"transfer impact assessment"**, the parties should take into account, in particular, the specific circumstances of the transfer (e.g. the

categories and format of the data, the type of recipient, the economic sector in which the transfer occurs, and the length of the processing chain) and the laws and practices relevant in this context. The latter assessment includes the applicable limitations and safeguards with a view to determine in particular whether the laws and practices do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR (in which case they will not be considered as affecting compliance with the SCCs).

As regards the impact on compliance with the SCCs, the parties **may consider different elements** as part of an overall assessment (see Clause 14, Footnote 12); such as 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. **In case of a negative assessment**, the parties may only transfer data based on the SCCs if they put in place **additional ("supplementary") safeguards** (e.g. technical measures to ensure data security, such as e.g. end-to-end encryption) that address the situation and thus ensure compliance with the Clauses. The same applies if the data exporter later on becomes aware that the data importer is no longer able to comply with the SCCs, including following a change in the laws of the third country. The data exporter will be required to suspend the transfer if it considers that no appropriate safeguards can be ensured, or if so instructed by the competent supervisory authority.

The SCCs (Clause 14) should not be read in isolation, but **should be used together with the detailed guidance prepared by the European Data Protection Board (EDPB)**. See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021) (available at: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf). The Recommendation contains a step-by-step roadmap for the assessment stage, a list of possible sources of information for that assessment (Annex 3) and various examples of supplementary measures (Annex 2).

41. To what extent does the data importer have to inform the data exporter about requests for disclosure it receives from public authorities (e.g. criminal law enforcement or national security authorities)?

First, the SCCs contain **requirements for the data importer to inform about government access** (either upon request or directly) to the data that has been transferred.

According to Clause 15.1, the data importer should promptly notify the data exporter if it receives a **legally binding request** from a public authority or court in the third country to disclose the personal data transferred. Similarly, it should notify the exporter if it becomes aware of any **direct access** (e.g. interception) by public authorities to such data. In this respect, the SCCs take into account that the **data importer may be prohibited by its national law** to provide (certain) information to the data exporter. In particular, if the data importer is not allowed to notify about specific instances of government access, it should use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. In case the data exporter is itself a processor, it has to forward the notification to its controller.

In addition, the **data importer should provide the data exporter at regular intervals with aggregate information** about access requests it has received (Clause 15.1(c)). This obligation again only applies **if the importer is allowed under its national law** to provide such information. In case the data exporter is itself a processor, it shall forward this information to its controller.

Second, the SCCs contain **additional notification requirements** in case the data importer becomes subject to **laws and/or practices that prevent it from complying** with the Clauses.

According to Clause 14(e) the **data importer agrees to notify the data exporter** promptly if, after having agreed to the Clauses and for the duration of the contract, it has reason to believe that **it is or has become subject to laws or practices not in line with the requirements under Clause 14(a)**. This includes situations where the laws of the third country change after the initial assessment, or where the data importer becomes subject to a measure (such as a disclosure request) in the third country that indicates an application of such laws in practice that is not in line with the initial assessment. In case the data exporter is a processor acting on behalf of a controller, it will have to forward the notification to its controller.

The SCCs again **take into account that the data importer may not be allowed** under its national law to inform about specific government access requests/direct access. In particular, Clause 16(a) contains a general notification requirement, according to the **data importer must promptly inform the data exporter** if it is **unable to comply** with the Clauses, **for whatever reason**. By relying on this Clause, the data importer has to inform the exporter that it can no longer comply with the SCCs without necessarily having to give specific information on government access. The data exporter will then be in a position to take the necessary measures, including possible suspension of the transfer or termination of the SCCs.

42. Does the data importer have to inform individuals about requests for disclosure received from a public authority? What if the data importer is prohibited from providing this information under its national law?

In accordance with Clause 15.1(a), the **data importer has to notify the concerned individuals** if it receives a **legally binding request** from a public authority or court in the third country to disclose personal data concerning them. In addition, it should notify the exporter if it becomes aware of any **direct access** (e.g. wiretapping) by public authorities to such data. At the same time, the **SCCs take into account that providing this information may not be possible, for legal or practical reasons.**

In particular, **the data importer may be prohibited** (by its national law) to notify about specific instances of government access. In this case, it should use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible.

In addition, **it may be difficult in practice** to contact the concerned individuals (e.g. because the data importer has no direct relationship with the individuals). In this respect, Clause 15.1(a) makes clear that the data importer may use the help of the data exporter (who may have a direct relationship with the individuals).

43. Is the data importer contractually required to challenge each request for disclosure it receives from a public authority?

No. According to Clause 15.2 of the SCCs, the data importer **has to review** whether the requests it receives are lawful under the applicable domestic legal framework. If the importer considers that there are **reasonable grounds to consider the request unlawful** (e.g. if it is evident that the requesting authority has exceeded its powers), it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are **sufficient grounds to appeal** the outcome of the procedure in first instance, such appeal should be pursued.

44. Is there a need to comply with Section III of the SCCs when relying on Module 4?

Section III of the SCCs contains a specific exception where Module 4 is used by an **EEA processor to return data it has received from its non-EEA controller** to that controller. In this scenario, the personal data was originally processed outside the EEA, where it was already subject to the domestic legal framework. There is therefore no need for the parties to carry out a "transfer impact assessment" (Clause 14) or comply with the obligations concerning access by public authorities to the data (Clause 15).

Example: a Moroccan company uses cloud services offered by a Luxembourg company to store data on its customer database. The SCCs (Module 4) can be used to transfer the data from Luxembourg (by the data exporter) back to Morocco (to the data importer). Since the data exporter is only sending back the data it has received from Morocco, it does not need to comply with Section III.

Conversely, the **exception does not apply** (and the parties therefore have to comply with Section III), **if the data that is transferred by the processor** (data exporter) to its controller (data importer) **also includes personal data originating in Europe**.

Example: a Chilean company instructs a Spanish processor to conduct market research and develop marketing material, using client data received from the Chilean company and client data it has collected in Spain. Module 4 of the SCCs can be used by the Spanish processor to transfer aggregated data on the two data sets to Chile. Since the data exporter is also transferring data collected in Europe (and not just the data it has received from Chile) to the data importer, it has to comply with Section III. This applies to the entire dataset that is transferred to Chile (i.e. both the data received from Chile and the data collected in Spain).