Standard Data Protection Clauses

Explanatory Note to the draft of the SDPC according to Art. 46 (1) GDPR

Edition May 2020

SCOPE EUROPE

General Information

Authors and Special Thanks

SCOPE Europe, with special thanks to
Frank Ingenrieth LL.M., Cornelius Witt, Julia Casella, Carolin Rost.

Drafting these SDPC, SCOPE Europe has been supported by
RA Daniel T. Kühl, https://paxaru.com
Prof. Dr. Gerald Spindler, Chair of Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law, University of Göttingen.
Anna Zsófia Horváth, Research Assistant at Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law, University of Göttingen.
Stakeholders and industry associations providing helpful feedback to prior versions of this draft.

Project Website / Further Information

https://scope-europe.eu/sdpc.

Project lead

SCOPE Europe bvba/sprl

Associated companies:

Alibaba Cloud (Singapore) Private Limited, DATEV eG, eyeo GmbH (until October 2019), Fabasoft AG and SAP Belgium NV/SA

Copyright/Imprint

SCOPE Europe sprl
Rue de la Science 14
1040 BRUSSELS
https://scope-europe.eu
info@scope-europe.eu

Managing Director
Jörn Wittmann

Company Register: 0671.468.741
VAT: BE 0671.468.741

Credits

Front-Picture: Photo by Andrew Butler on Unsplash.

Version 1.0 (June 2019): initial draft publication, request for public feedback.
Update July 2019: minor adjustments of notation of associated companies.
Update October 2019: official publication of final draft, incorporating public feedback and minor editorial adjustments.
Version 2.4 (May 2020): clarifications, especially regarding “re-transfer” into EEA.

1 Intent of this note

This note serves as an introduction for the main purpose, scope and general approach of the draft of the Standard Data Protection Clauses (SDPC). It outlines and explains the background of this initiative, key principles of the chosen structure as well as legal issues that were considered while drafting these SDPC. This explanatory note only covers general remarks on the methodology and structure of the SDPC. More detailed explanations for each provision can be found in the draft as is appropriate. To keep it lean, though, both documents focused on main arguments, for even more detailed information please reach out to the initiative[1].

This note shall be considered as an accompanying document for the draft of the SDPC. It refers to definitions outlined in Clause 1 of the SDPC. All terms defined for the first time in the SDPC will be referenced throughout the SDPC in ***Capital Bold and Italic Font*** as terms defined within Art. 4 GDPR and incorporated into these SDPC will be referenced in *small italic font*.

2 Background

Due to the current lack of SDPC according to Art. 46 (1) GDPR, the development of a draft set of clauses was initiated by a consortium of different European and international companies[2].

Currently there is a lack as SDPC have not been adapted to GDPR yet, so clauses currently in use still reflect directive requirements. Additionally, clauses specifically addressing the needs of processor-to-processor environments are missing. And lastly, the approach of current clauses by expecting at least one party to be exporting does not reflect (European) business needs and modern business models where personal data may be leaving and (re-)entering the EU through a processing chain. By drafting these SDPC, those issues were key to be reflected.

Hence, before drafting, an extensive review of existing literature and academic works was conducted to evaluate the current status quo. Further, the benefits and disadvantages of the WP 29 draft[3] were examined. Also, on-going consultation with different stakeholders and partners from industry (including associations representing diverse memberships with different processing activities, business models and company structures, including many small and medium-sized enterprises) and from the

[1] For more details or feedback, please reach out to us via https://scope-europe.eu/sdpc.
[2] This initiative was sponsored by Alibaba Cloud (Singapore) Private Limited, Datev eG, eyeo GmbH (Adblock Plus), Fabasoft AG and SAP Belgium NV/SA.
[3] Working document 01/2014 on Draft Ad hoc contractual clauses “EU data processor to non-EU sub-processor", accessed on 20 May, 2019: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf.

legal sphere (such as law firms specialized on data protection and IT-law) ensured to meet existing market needs. In this context, this draft of SDPC intends to be as comprehensive and accurate as possible – e.g. by avoiding redundant regulations and reducing complexity – in order to enhance wide market adoptions while simultaneously safeguarding a high level of data protection for ***Third Country*** transfers.

3 Key principles

3.1 Purpose of this SDPC draft

This draft of SDPC requires that, in order to perform a ***Third Country*** sub-*processing* of *personal data,* the ***Parties*** concerned need to agree upon three legal components:

- The ***Data Processing Agreement*** or ***Sub-Processing Agreement*** (according to Art. 28 GDPR),
- the relevant technical and organizational measures (TOMs) and
- the SDPC Agreement.

Legally, it is up to the ***Parties*** whether they agree upon each component separately or by any combination thereof. Whereas the first two components are always mandatory for legal *processing* of *personal data* by a *processor*, the SDPC provide safeguards for transferring *personal data* to a ***Third Country*** (Art. 46 (1) GDPR). To date, no SDPC specifically designed to address transfers of *personal data* between a *(Sub-)processor* and another *Sub-Processor* to or within a ***Third Country*** have been adopted. This draft of SDPC has been developed to provide safeguards for the transfer of *personal data* from one *processor* to another where the *processing* of *personal data* affects ***Third Country*** transfers.

3.2 Implementation of these SDPC

The development of this draft of SDPC is driven by the goal of achieving a high-level of comprehensibility and accuracy as well as the desire to avoid redundant regulations (e.g. to GDPR, ***Data Processing Agreements*** and ***Sub-Processing Agreements***).

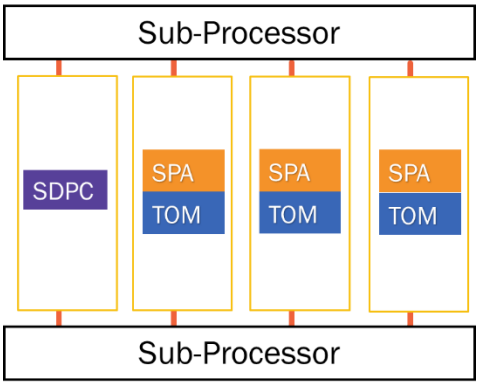
Therefore, the draft deems it important that a ***Data Processing Agreement*** or ***Sub-Processing Agreement*** and the ***SDPC Agreement*** are handled as separate as possible. The SDPC shall only provide provisions addressing transfers to or within a ***Third Country***. As mentioned above, the ***Data Processing Agreement*** or ***Sub-Processing Agreement*** are always necessary to process *personal data* by a *processor*, no matter if transfers to a ***Third Country*** are involved. The implementation of TOMs and the security of the technology is important for the processing of *personal data*, but it is not coming

up with the question of transfers of *personal data* to or within a **Third Country**. Hence, the question of TOMs should be addressed as part of a ***Data Processing Agreement*** or ***Sub-Processing Agreement***.

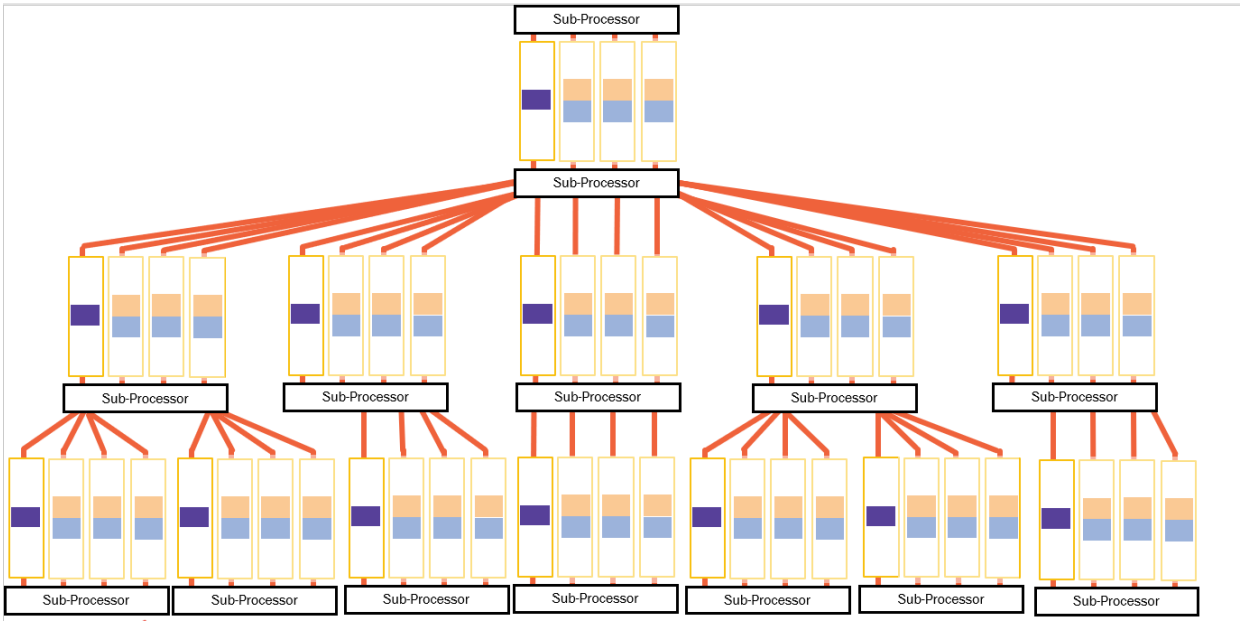
This means, that for the sake of clarity and unambiguity, clauses subject to the ***Sub-Processing Agreement*** and (or, where relevant ***Data Processing Agreement***), as well as TOMs are left out from the SDPC:

Again, to avoid duplication, the SDPC refer to the ***Sub-Processing*** or ***Data Processing Agreement*** and the TOMs within some of its clauses; repetitive regulations are limited to those provisions that require modification or addition. By this, the SDPC aim to achieve a high degree of comprehensibility fostering their practical implementation in small and medium-sized organizations, also.

Splitting up the necessary components in two contracts between *the Parties* allows for the possibility to agree on different independent ***Sub-Processing Agreements*** and TOMs (e.g. when there are different "qualities" of *personal data* handled regarding sensitivity), which, when ***Third Country*** transfers are wished for, can then refer to the SDPC.



A key benefit to this approach is, that a change to the SDPC by the European Commission principally will not affect the contract of the ***Sub-Processing Agreement*** and the TOMs. This reduces an administrative overhead per contract and raises focus on individual processing related measures, as the following graphic shows:



A change to the SDPC would then only cause for a need to change the highlighted contracts (the SDPC), the different ***Sub Processing Agreements*** (or where relevant ***Data Processing Agreements***) can remain unchanged.

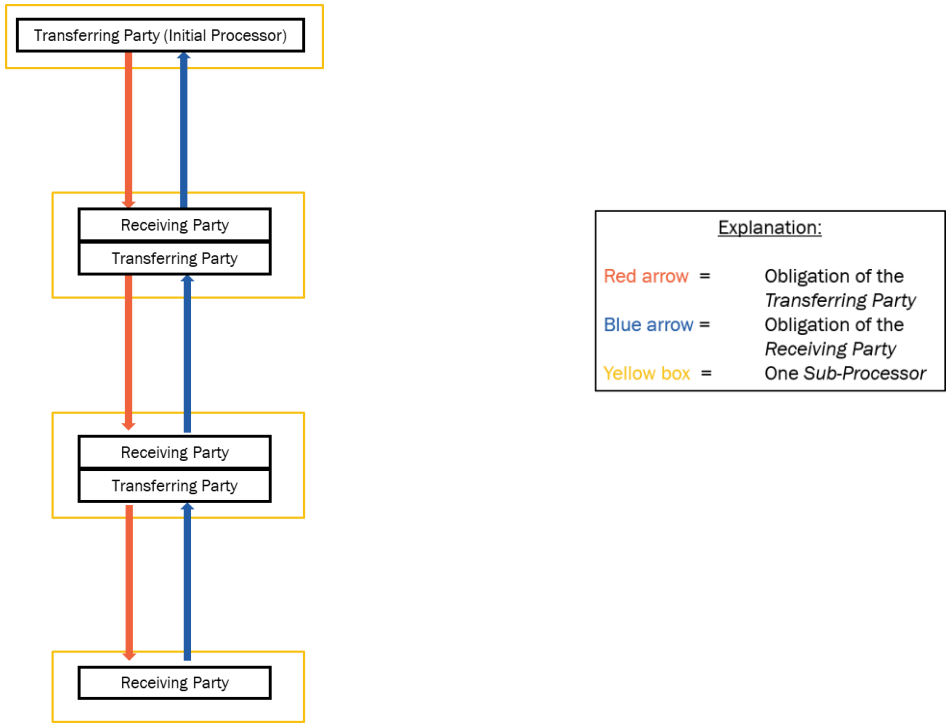
At the same time, the separation between the SDPC and ***Sub-Processing Agreement*** or ***Data Processing Agreement*** and the TOMs creates a high degree of flexibility for companies adopting the clauses. For instance, *processors* are free to use different compliance schemes as an element by which to demonstrate sufficient guarantees under the ***Sub-Processing Agreement*** or ***Data Processing Agreement,*** specifically regarding the TOMs (e.g. an approved Code of Conduct as referred to in Art. 40 GDPR or an approved certification mechanism as referred to in Art. 42 GDPR) while referring to the SDPC for ***Third Country*** data transfers.

3.3 Chain approach of these SDPC

The common terminology and mechanism of “Data Exporter” and “Data Importer” do not address those circumstances where a ***Sub-Processor*** in a ***Third Country*** transfers *personal data* to a further ***Sub-Processor*** within the same country or to any other ***Third Country***. Therefore, this draft introduces

the terms "***Transferring Party***" and "***Receiving Party***." This literal adjustment allows the SDPC to safeguard all transfers - to or within a ***Third Country*** - regardless of whether the *personal data* is actually exported from the EU in the respective data transfer. Moreover, this draft refers to all ***Sub-Processors*** as a ***Transferring Party*** or ***Receiving Party***.

Due to this chain-approach, each ***Sub-Processor*** is principally both ***Receiving*** and ***Transferring Party***. Exceptions are only the ***Initial Processor***, which lacks the receiving element under the SDPC, and the last ***Receiving Party***, which lacks the transferring element. Understanding this dual role is key for the understanding of the SDPC.



Due to this chain approach, each ***Sub-Processor*** is bound to the obligations of the ***Receiving Party*** and the ***Transferring Party***, depending on the function he is executing. This also allows for the SDPC to accurately portray the complex contractual relations in a processing chain where various ***Sub-Processors*** are involved.

4 Implemented safeguards

In the following, some provisions of the SDPC are exemplarily introduced to illustrate how appropriate safeguards for ***Third Country*** transfers were incorporated. None of the following mechanisms creates an appropriate safeguard by itself, however all provisions in their entirety and correlation to each other achieve the adequate level of *data protection* for ***Third Country*** transfers. It is therefore crucial to

understand the intent of the following, major single provisions as relevant contribution to the overall goal.

4.1 Rights and Obligations of the Parties

The main safeguards are found in various obligations of and rights for the ***Transferring Party*** and the ***Receiving Party***:

Principally, the draft distributes each obligation of *the* ***Parties*** to the one most concerned and with *processing* closest related. For example, as it is the ***Transferring Party*** that decides to engage a further ***Sub-Processor***, it is the ***Transferring Party*** which is most concerned to establish the legal basis for this engagement. Therefore, it is the obligation of the ***Transferring Party*** to have a ***Data Processing Agreement*** (where the ***Transferring Party*** is the ***Initial Processor***) or a ***Sub-Processing Agreement*** in place. Also following this logic, the ***Transferring Party*** shall secure ***Written*** prior authorization for transfers of *personal data* in general and specifically for performing transfer of *personal data* to ***Third Countries***.

The rights or obligations of the ***Parties*** are, in order to keep the SDPC lean and short, not accompanied by a specific corresponding obligation of the respective other ***Party***. For example, the ***Receiving Party*** has the right to pose a reasonable ***Written Request*** towards the ***Transferring Party*** to provide sufficient information and documentation to demonstrate its compliance with applicable legal and contractual obligations. There is no necessity for a corresponding individual obligation of the ***Transferring Party*** as the ***Party*** subject to such a ***Request*** is already obliged to properly respond to any ***Requests***.

One exception to this principal of fully separated obligations is the applicable law for the ***Receiving Party***, as this does not relate to one ***Party*** only. On the one hand, it is the ***Transferring Party's*** decision to engage a specific ***Sub-Processor*** and therefore it should beforehand assess the applicable law for this ***Receiving Party*** and reasonably conclude that the applicable law does not conflict with the ***Transferring Party's*** obligations under the ***Sub-Processing Agreement*** and the ***Applicable Data Protection Law***. On the other hand, the ***Receiving Party*** knows its "own" applicable law best, and is therefore obliged to cooperatively assist the ***Transferring Party*** in its assessment. The ***Receiving Party*** also has to inform the ***Transferring Party*** about the possibility of requests of disclosure regarding *personal data processed* by the ***Receiving Party*** by competent law enforcement authorities as well as any changes to the applicable law. In this regard, the obligations of the ***Transferring Party*** and the ***Receiving Party*** necessarily complement each other.

Further safeguards, implemented by the rights and obligations for the ***Parties*** are, e.g.:

- the assessment of the ***Transferring Party*** about possible bilateral agreements on the enforcement of judicial rulings – none of the other safeguards will be effective, if the SDPC and any rights and obligations therein cannot be enforced;

- upon ***Request***, the disclosure of the ***Transferring Party*** to the ***Receiving Party*** of the relevant section of its ***Sub-Processing Agreement*** in its role as a ***Receiving Party*** – principally control and trust is enabled from top-to-bottom, however there might be circumstances where parties within the chain become doubtful about the legitimate *processing*, so that the SDPC provide a moderate bottom-to-top mechanism;

- transparency duty of the ***Receiving Party*** towards the ***Transferring Party*** regarding implemented technical and organizational measures – the essence of control requires more than simply signing contractual agreements, but also requires appropriate possibilities to perform due diligence and verify compliance;

- notification duty of the ***Receiving Party*** towards the ***Transferring Party*** in e.g. cases of conflicting ***Instructions*** of the *controller* and the ***Sub-Processing Agreement***, cases of conflicting ***Instructions*** and the legislation applicable, *personal data breaches* and legally binding requests of disclosure – the chain approach is based on compliance and trust. In case there might be some inconsistency in practice, transparency and notification duties shall ensure respective trust between the ***Parties***;

- information duty on engaging further ***Sub-Processors*** by the ***Receiving Party*** – a re-confirmation on principles of Art. 28 GDPR and pre-requisite to establish a chain approach at all*;*

- effective third party beneficiary rights for *data subjects* and *controllers* – safeguarding that control stays intact throughout the chain, even where things have been going wrong;

- determination of European Courts and European governing laws for the execution of SDPC and third party beneficiary rights thereunder – SPDC are a contractual framework to safeguard European principles whilst *personal data* is transferred internationally. It was considered key that European governing law and competent courts will enforce such a framework.

4.2 Implementation of technological and organizational measures pursuant Art. 32 GDPR

The draft does not include a provision stipulating concrete TOMs. As explained above, the question of TOMs should be addressed in the ***Sub-Processing Agreement*** or ***Data Processing Agreement***. Nevertheless, the SDPC oblige the ***Parties*** to sign an agreement or ensure the existence of any other

legally binding act pursuant to Art. 28 GDPR (see clauses 3 (2) and (3) of the SDPC). This includes the stipulation that the *processor* implements appropriate technical and organizational measures that ensure a level of security that is appropriate to the existing risk. Specifying requirements for TOMs that would fit every industry use case and business need proved difficult. Therefore, technical and organizational measures include both, those being required by the respective ***Sub-Processing Agreement*** or the respective ***Data Processing Agreement*** (where the ***Transferring Party*** is the ***Initial Processor***) (see Art. 28 (3) GDPR), and those being required by the ***Applicable Data Protection Law*** (Art. 32 GDPR). Furthermore, the ***Receiving Party*** is obliged to provide upon ***Request*** to the ***Transferring Party*** relevant documentation that demonstrates the sufficient implementation of technical and organizational measures. By that mechanism, the SDPC provide, in case of a failure of the ***Data Processing Agreement*** or ***Sub-Processing Agreement***, a safety net which the ***Parties*** can rely on. Also, as the SDPC only require that the level of protection of GDPR is maintained when *personal data* is transferred into a ***Third Country***, it is considered sufficient to implement the obligation to take into account Art. 32 GDPR to ensure the appropriate level of protection of the *data subject* in the event of transfers to or within a ***Third Country***.

4.3 Third-party beneficiary rights

According to Art. 24 (1) GDPR, the *controller* is obliged to exercise control over the *processing* in the *processing* chain. Safeguarding this obligation in cases of ***Third Country*** transfers of *personal data*, the SDPC grant the *controller third-party* beneficiary rights, equivalent to those set by GDPR. The same concept applies to *data subjects* which are also granted third party beneficiary rights, as the protection of the rights and freedoms of data subject is the overall principle and intent of GDPR. This means, that the *controller* and the *data subject* are entitled to enforce *third-party* beneficiary rights as they are set out in clause 6 against the ***Parties***. For the *third-party* beneficiary rights of the *controller* this means that the ***Receiving Party*** must fulfill its obligations towards the *controller* pursuant Clause 4 (11) of the SDPC, as if the *controller* was the ***Transferring Party***. The *controller* is also entitled to terminate the transfer, if the ***Receiving Party*** does not fulfill its obligations, or, if the ***Receiving Party*** informs the *controller* about circumstances that jeopardize the appropriate level of protection for the *processing* of *personal data*. For the *data subjects*, it is ensured that they have the possibility to approach to any *processor* directly in case the primary point of contact (the *controller)* has factually disappeared or has ceased to exist in law.

4.4 Termination of transfers

The SDPC focus on the transfer as such, as the transfer is – by law – the risk enhancing process. In other words, *personal data* are not protected if, in case of any infringements or reasonable doubts

against any ***Party***, the contractual framework will be terminated, as this will not directly affect the *processing* of *personal data*. Therefore, the SDPC require any transferring and *processing* to be terminated in such cases, which means that *personal data* must be deleted or returned and deleted.

5 Models of execution & Related aspects

5.1 Formalities

As explained above, one of the key principles of these SDPC is to keep the ***Sub-Processing Agreement*** or ***Data Processing Agreement*** separated from the SDPC. To illustrate this approach, the draft includes his own rubrum and signature. The idea is to allow for the SDPC to be a standalone contract. Nevertheless, the SDPC themselves – meaning the provisions – can of course be incorporated in the ***Sub-Processing Agreement*** or ***Data Processing Agreement***. However, the provisions of the SDPC must not be adversely modified in those cases. This might be more effective for a *processor*-to-*processor* relation which don't consist of various ***Sub-Processing Agreements***. However, such deviations would then mean, that the advantages pointed out under Chapter 3.2 of this note would be omitted. The SDPC does not provide any provisions yet regarding the actual form of signature that is required (e.g. wet signature or electronic form). The rubrum and signature field are for illustration purposes only. From a practical perspective, any signature that meets the requirements of ***Documented*** in the sense of the SDPC should suffice and to reflect highly complex chains, electronic means are likely.

5.2 Variation of Contract

In some cases, a ***Sub-Processing Agreement*** or ***Data Processing Agreement*** can be signed precautionary, without obligations under GDPR. For instance, this could be the case if a party outsources certain maintenance or similar services which are not primarily related to the *processing* of *personal data*. Subsequently, the SDPC can be signed precautionary as well. As the ***Parties*** in those cases are going beyond their legal requirements already, the SDPC offer them the possibility to reduce administrative burdens whilst any modification of core principles is still prohibited.

5.3 Stipulations on special data protection legislation

Within these SDPC there are several references to ***Applicable Data Protection Law***, which acts as a reference to GDPR. The idea is to keep the SDPC as simple and lean as possible, and to, for the moment, externalize possible ambiguities resulting of national law of the member states providing additional data protection requirements to the ***Data Processing Agreement*** or the ***Sub-Processing Agreement***. A reflection in the SDPC of these additional requirements would create a very high level of complexity. Furthermore, in most common cases, GDPR already provides a high level of data protection, which is considered to be sufficient regarding the safety of freedom and rights of *data*

subjects. This raises the question to which extent the reflections of additional data protection requirements are necessary and would justify the above-mentioned higher complexity. Nevertheless, by extending the definition of ***Applicable Data Protection Law*** in the draft (Provision 1 (1) g), such a reflection could be made. For the moment it is expected that requirements of any national law will necessarily be reflected in the ***Data Processing Agreement*** or ***Sub-Processing Agreement***, anyways.

6 Further Consideration

6.1 Independent supervision of compliance with SDPC

An additional safeguard could be to incorporate provisions governing the role of a monitoring body or a comparable entity. Such a body would monitor the *processors* and ensure their compliance with the SDPC. Of course, such aspects would need to be intensively discussed. But in order to achieve the goal of enhancing the practical implementation of the SDPC by this mechanism, such a body must add a value to the execution of this SDPC and not only limit itself to revising legal formalities. Furthermore, it is worth pointing out that this would create an additional layer of complexity to this draft of clauses that would affect its length and comprehensibility. Therefore, the implementation of establishing a monitoring scheme was not introduced in these SDPC as of now. The implementation of such a body seems not relevant for the establishment of a credible and effective safeguard, yet, but rather should be considered in future discussions and developments especially depending on future ECJ rulings in this regard.

6.2 Possibilities of expanding the scope of application of these SDPC

Currently these SDPC are applicable from the ***Initial Processor*** – the first ***Transferring Party*** – to the last ***Sub-Processor*** of the *processing* chain, the last ***Receiving Party***. This means, that up to now, the SDPC are only designed to be implemented in the *processor*-to-*processor* context. Nevertheless, the applicability could be easily adjusted, by incorporating *controller* to *processor* relationships as well. Such an adjustment would only require the extension of the current *processor*-to-*processor* approach by one “chain link”.

The underlying principle, namely the chain approach and separation of all three main components for ***Third Country*** transfer (see Chapter 3 of this Explanatory Note), may work equivalently in other *processing* contexts as well, e.g. the *controller*-to-*controller* context, and for joint controllerships and hence even controller-to-controller- and joint-controller-to-*processor* context. Adjusting the current draft accordingly would allow the SDPC to work like an assembly kit, providing different kit components, which can be chosen by the two parties concerned.