Standard Data Protection Clauses

Draft and Explanations

Edition May 2019

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 (Adblock Plus), 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.

Standard Data Protection Clauses

Draft and Explanations

Company Name:

Address:

Tel.:

fax:

e-mail:

Other information needed to identify the organization:

(Hereinafter, the **Customer**), as the *Transferring Party*

And

Company Name:

Address:

Tel.:

fax:

e-mail:

Other information needed to identify the organization:

(Hereinafter, **Provider**) as the *Receiving Party*

each a "**Party**"; together "**the Parties**",

HAVE AGREED on the following Standard Data Protection Clauses (hereinafter "SDPC"), in order to adduce appropriate safeguards according Art.46 (2) lit. c) General Data Protection Regulation (hereinafter "GDPR") with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer of *personal data* by the *Transferring Party* to the *Receiving Party*.

Clause 1 Definitions

(1) The definitions of GDPR Art. 4 shall apply to these SDPC;	In order to keep the SDPC short and comprehensible, these SDPC mainly rely on the definitions provided in the GDPR. Therefore, any term defined in the GDPR has the same meaning here. These SDPC provide additional definitions as necessary to complement the GDPR. These additional definitions help address the possibility of a processing chain that includes more than one *processor* or several *Sub-Processing Agreements*. In order to have specific references, further definitions have been added.
a) "*Initial Processor*" means the *processor* directly engaged by the *controller*;	Because the GDPR does not differentiate between different *processors* within processing chain, the terms "*Initial Processor*" and "*Sub-Processor*" have been added to clarify this division of roles.
b) "*Sub-Processor*" means any *processor* subsequent to the *Initial Processor*;	
c) "*Transferring Party*" means any *processor* who transfers *personal data* to the *Receiving Party*;	In contrast to the draft of the WP29, "*Transferring Party*" and "*Receiving Party*" do not only refer to a *processor* in the EU who transfers *personal data* to a *Sub-Processor* in a *Third Country*. They also incorporate a *processor* that transfers *personal data* from a *Third Country* onward to another *Sub-Processor*.
d) "*Receiving Party*" means any *Sub-Processor* engaged by a *Transferring Party* who agrees to receive *personal data* from the Transferring Party intended for *processing* on behalf of the *controller*;	
e) "*Data Processing Agreement*" is any agreement according to GDPR Art. 28 (3) between the *controller* and the *Initial Processor;*	The *Data Processing Agreement* is a prerequisite to the lawful *processing* of *personal data* which also serves to define the main purposes and means of the *processing*. Many rights and obligations of *the Parties* included in these SDPC may be derived from this agreement. Accordingly, it is crucial to provide a definition for such agreements.

f) "*Sub-Processing Agreement*" means any processing agreement between two *processors* according to Art. 28 (4) GDPR;	The term "*Sub-Processing Agreement*" refers to all *processor*-to-*processor* processing agreements in the processing chain. Although the GDPR provides requirements for such agreements in Art. 28 (4), it does not explicitly provide a definition of these agreements.
g) "*Applicable Data Protection Law*" means the European General Data Protection Regulation (GDPR) 2016/679, as amended;	Within these SDPC there are several references to *Applicable Data Protection Law*. As these SDPC govern *Third Country* transfers there may be ambiguities regarding the applicable law. Hence, this definition clarifies that – for these SDPC – the *Applicable Data Protection Law* shall be the GDPR. For the avoidance of doubt: there may be cases that national law of the member states provides additional requirements. Such additional requirements are not reflected by these SDPC as such reflection would create a very high level of complexity. These SDPC provide an adequate level of data protection as required by GDPR. If any national law provides additional requirements those should be reflected by the *Data Processing Agreement* or *the Sub-Processing Agreement*. As this approach may change, though, in future, this definition eases future adjustments by simply extending the scope of this definition.
h) "*Instruction*" is a *Documented* order of the *controller* or the *Transferring Party* related to the *processing* or transfer of *personal data* in accordance to Art. 28 (3) lit. (a) GDPR that is covered by and made in accordance with these SDPC, *Sub-Processing Agreement*, the *Data Processing Agreement* or *Applicable Data Protection Law*;	The term *Instruction* was added to simplify the references to the rights and obligations of *the Parties.*
i) "*Third Country*" means any country or international organization as described in Chapter V of GDPR;	The same rules apply to the transfer of *personal data* to *Third Countries* and *international organizations* within the provisions of these

	SDPC. So, both are covered by this term to keep the SDPC as lean and simple as possible.
j) *"Request"* means a demand by a *Party* or the *controller* from a *Party* requiring information related to the *processing* of *personal data* that is covered by and made in accordance with these SDPC, *Sub-Processing Agreement,* the *Data Processing Agreement* or *Applicable Data Protection Law* to the extent applicable to the *processing of personal data* to which the demand relates*;*	
k) "*Written*" and "*Documented*" by any auditable means, including electronic means, e.g. emails, dashboards and related log files.	
(2) Terms defined by these SDPC will be referenced in *Capital Italic Font*. All terms defined within Art. 4 GDPR and incorporated into these SDPC will be referenced in *small italic font*.	
(3) Whenever there is a reference to an Article of GDPR, this shall stipulate the applicability of such Articles irrespective of their applicability under Art. 3 GDPR.	

Clause 2 Rights of the Transferring Party

(1) Regardless of any rights under the *Data Processing Agreement* and the *Applicable Data Protection Law* the *Transferring Party* shall additionally have the rights as set out in these SDPC and especially in this Clause.	The *Transferring Party* must ensure the GDPR compliance of its contractual partner (i.e. the *Receiving Party*). For this purpose, the *Transferring Party* needs certain adequate rights against the *Receiving Party*. The following provisions describe and ensure such rights.
(2) The *Transferring Party* may transfer any *personal data* to the *Receiving Party* within the	

framework of the *Sub-Processing Agreement* or the *Data Processing Agreement*, as applicable.	
(3) The *Transferring Party* is entitled to give any *Instruction* to the *Receiving Party* within the framework of the *Sub-Processing Agreement*, the *Data Processing Agreement* and the *Applicable Data Protection Law*.	
(4) The *Transferring Party* is entitled to receive upon *Request* any relevant information from the *Receiving Party* to verify the *Receiving Party's* compliance with these SDPC, the *Sub-Processing Agreement* and the *Applicable Data Protection Law*. Where and insofar as the *Sub-Processing Agreement* governs modi operandi of the right to audit under Art. 28 GDPR, such modi operandi shall prevail.	Hereby the *Transferring Party* is enabled to oversee the *Receiving Party's* compliance by receiving relevant information. Based on this information the *Transferring Party* may conclude its further actions. A corresponding obligation for the Receiving Party to properly deal with such *Requests* is provided in 4 (5). This is not an explicit Right to Audit with a possibility to perform onsite audits. Again, principally any provisions of such kind are expected to be reflected in the *Data Processing Agreement* or *Sub-Processing Agreement*. This provision simply reassures that – in lack of any provisions within any such agreements – at least a minimal safeguard is in place. Realistically one must understand "any relevant information" as comprising both "documents" and – where relevant – also access to the premises to verify compliance.

Clause 3 Obligations of the Transferring Party

(1) The *Transferring Party* agrees and warrants to fulfil the obligations as set out in this Clause.	These SDPC strive to be lean and simple. To reach this goal these SDPC strictly follow a chain-approach. Hence a *Transferring Party* may also be a *Receiving Party* in another contractual relationship. The obligations of the *Transferring Party* are hence limited to those being necessary obligations whilst preventing unnecessary duplicates with the obligations of the *Receiving Party*.

(2) The *Transferring Party* shall take reasonable measures designed to ensure that all *processing* of *personal data* is subject to either a *Data Processing Agreement* or a *Sub-Processing Agreement.*	A *Data-Processing Agreement* or a *Sub-Processing Agreement* is a requirement for *processing personal data* under these SDPC and the GDPR. The SDPC shall provide an additional framework regarding *Third Country* transfers. So, the *Data Processing Agreement* or *Sub-Processing Agreement* shall govern the mere *processing* and its requirements itself, whereas the SDPC govern *Third Country* transfers. The strict separation of both was a main goal of these SDPC. However, besides signing a *Sub-Processing Agreement* with its *Sub-Processors*, the *Transferring Party* shall take reasonable measures to ensure that the processing chain is not interrupted. This includes a due diligence in both directions: the processing chain down- and upwards. For the latter the SDPC provide supporting rights of *Receiving Parties*, see Clause 3 (12) and Clause 5 (2).
(3) The *Transferring Party* shall have entered into an effective *Sub-Processing Agreement* with the *Receiving Party* for the duration of the *processing* of *personal data* on behalf of the *controller* under these SDPC; any terms and conditions of such *Sub-Processing Agreement* must not be less protective than the terms and conditions agreed in the *Data Processing Agreement* or any applicable *Sub-Processing Agreement* the *Transferring Party* is subject to.	These SDPC work in conjunction with the *Sub-Processing-Agreement* that is demanded by GDPR. To ensure that *the Parties* have this obligation, even outside of the territorial scope of the GDPR, this provision requires a *Sub-Processing Agreement* to be signed between *the Parties.* The *Sub-Processing Agreement* together with these SDPC shall provide the adequate level of data protection required for a *Third Country* transfer of *personal data*. Further, the requirement of an effective signed *Sub-Processing Agreement* ensures that *the Parties* have agreed upon technological and organizational measures appropriate to the risk according Art. 32 GDPR.
(4) The *Transferring Party* shall have a prior *Written* authorization of the *controller* or its *Transferring Party* to transfer *personal data* to the *Receiving Party.*	This provision refers to Art. 28 (2) GDPR, requiring an authorization of the *Transferring Party* to initiate further sub-*processing*. Without prior authorization, the *Transferring Party* must not transfer *personal data* to the *Receiving Party*.

(5) The *Transferring Party* shall have prior *Written* authorization and/or *Instructions* to transfer to and/or *process personal data* in a *Third Country*.	Having a sole authorization to engage a *Sub-Processor* is not sufficient to transfer *personal data* to or process *personal data* within a *Third Country*. Hence, it is required, that the *Transferring Party* has prior *Written* authorization and/or any *Instruction* to transfer to or process *personal data* within a *Third Country*.
(6) The *Transferring Party* shall assess whether there is any bilateral agreement on the enforcement of judicial rulings between a) the member state of the court competent according to Clause 10 (2) or Clause 10 (3); and b) the countries of any potential enforcements against the *Receiving Party*.	The limitation of the competent court to be within EU (as provided by Clause 10 (2) and (3)) shall safeguard an adequate interpretation of these SDPC in the light of GDPR and a European understanding of fundamental rights and freedoms of *data subjects*. In order to avoid that any decision against *Receiving Parties* become ineffective, it is necessary to also safeguard the enforcement of such judicial rulings. Any noncompliance of the *Transferring Party* with this provision is a breach of contract as noncompliance would abolish the safeguarding function of Art. 46 (2) GDPR and make the data transfers of *personal data* to a *Third Country* by the *Transferring Party,* without having other safeguards according to Art. 46 (2) GDPR in place, unlawful.
(7) The *Transferring Party* shall promptly forward the following information to the *Receiving Party* a) any received *Instructions*; and/or b) any received *Requests* from the *controller* relating to the *processing* by the *Receiving Party* under these SDPC;	These SDPC distinguish between *Instructions* and *Requests*. *Instructions* always relate to a certain handling of *personal data*, while *Requests* address a wider concept that encompasses all sorts of inquiries (e.g. and mostly to receive more substantive information). The purpose is to ensure that *Instructions* and/or *Requests* from the *controller* always reach the *Party* that the *Instructions/Requests* relate to. Hence, the *controller* stays in control over the *processing*. For the avoidance of doubt: GDPR follows the concept that all *processing* of *personal data* is determined by the *controller*, even if the *controller* engages a *processor*. This provision safeguards that any explicit *Request* or *Instruction* of

	the *controller* flows down the full processor chain, where applicable.
(8) The *Transferring Party* shall ensure that all its *Instructions* towards the *Receiving Party* are in accordance with or do not contradict any *Instructions* the *Transferring Party* received itself.	In practice *controllers* do not individually instruct every single measure or action within the processor chain. In fact, the *controller* and the *Initial Processor* agree upon the fundamental principles and level of security and data protection that the implemented technical and organizational measures shall safeguard. To reflect this approach, this provision ensures that, if the *Transferring Party* needs to instruct the *Receiving Party* (e.g. about a certain way to implement a given technological or organizational measure), the *Transferring Party* shall only issue *Instructions* that are in accordance with the *Instructions* that the *Transferring Party* has received itself. This provision thus ensures that *Instructions* must not originate from the *Transferring Party* that are not in accordance with the *Instructions* of the *controller* or any other *Transferring Party* – where the respective *Transferring Party* is a *Receiving Party* itself.
(9) The *Transferring Party* shall not transfer any *personal data* to the *Receiving Party* where such a transfer may conflict with any *Instruction*, the *Sub-Processing Agreement*, the *Data Processing Agreement* (where the *Transferring Party* is the *Initial Processor*) or the *Applicable Data Protection Law.*	This provision ensures that the *Transferring Party* always reassesses the transfer of *personal data* in order to avoid conflicts that may arise out of the transfer. Especially the *Transferring Party* needs to ensure that it has the authorization of the *controller* to transfer the *personal data* to another *Sub-Processor* in a *Third Country*. Even if there is a general authorization for engaging *Sub-Processors* and transfer to or within *Third Countries*, such authorization may be limited to specific *personal data*, or may require additional technical and organizational measures to be in place. This mandatory reassessment shall ensure that any such modifications and limitations of an authorization provided will be respected.

(10) The *Transferring Party* shall only engage the *Receiving Party* after assessing the applicable law for the *Receiving Party* and reasonably concluding that the applicable law does not conflict with the *Transferring Party's* obligations under the *Sub-Processing Agreement* and *Applicable Data Protection Law*.	The *Transferring Party* shall not only rely on information provided by the *Receiving Party* on this topic but have an original obligation on conducting on research and risk assessment. This obligation corresponds with the obligation of the *Receiving Party* Clause 4 (8)/(9).
(11) Where the *Transferring Party* is being notified by the *Receiving Party* about any potential conflicts according to Clause 4 (2) and (9), the *Transferring Party* shall re-assess and, if necessary, adjust its *processing* activities and implemented appropriate technical organizational measures as agreed upon in the *Sub-Processing Agreement* to leverage the risks related to the potential conflicts regarding the applicable law of the *Receiving Party*.	
(12) The *Transferring Party* shall promptly and properly deal with all *Requests* of the *Receiving Party* relating to the *processing* of the *personal data* subject to these SDPC, the *Sub-Processing Agreement*, and the *Applicable Data Protection Law; especially* the *Transferring Party* shall, upon *Request*, provide relevant sections of its *Sub-Processing Agreement* in its role as a *Receiving Party*, i.e. especially whether the *Transferring Party* in its role as a *Receiving Party* is authorized to engage Sub-Processors and to transfer to and/or *process personal data* in a *Third Country*, or regarding required technical and organizational measures.	This obligation corresponds with the right of the *Receiving Party* in Clause 5 (2).

Clause 4 Obligations of the Receiving Party

(1) The *Receiving Party* agrees and warrants to fulfil the obligations as set out in this clause.	The *Receiving Party* is the *Party* which is subject to the most obligations within the SDPC. Para. (2) provide obligations which have to be fulfilled before executing the SDPC. Paras. (4), (5), and (6) provide obligations which must be fulfilled when *processing personal data*. Para. (7) covers situations where the *Receiving Party* must notify the *Transferring Party* about certain circumstances. Para. (10) provides *processing* obligations as well as reporting obligations regarding the engagement of another *Sub-Processor* by the *Receiving Party*. Para. (11) governs the situation when the *controller* invokes its *third party* beneficiary rights. Para. (12) determines the obligations of the *Receiving Party* when the *Transferring Party* or the *controller* has factually disappeared or has ceased to exist in law.
(2) Prior to executing these SDPC and frequently during the term of these SDPC the *Receiving Party* shall assess the legislation applicable to it and has no reason to believe that this legislation conflicts with obligations provided by these SDPC, *the Sub-Processing Agreement*, the *Data Processing Agreement* and the *Applicable Data Protection Law*. Where there is an adequacy decision in place the assessment of conflict between these SDPC and the applicable law may be reduced to the finding of such adequacy decision; where such decision is declared void the *Receiving Party* must individually assess the legislation and reason why there is no conflict. For the avoidance of doubt: where an adequacy decision will be declared void, the *Receiving Party* may no longer reduce its assessment to the finding of such adequacy decision but must individually assess the legislation and reason why there is no conflict.	There might be cases where the national law of a *Third Country* contradicts the principles of these SDPC, the *Sub-Processing Agreement*, the *Data Processing Agreement* or GDPR. In such circumstances, the *Receiving Party* would be subject to conflicting obligations that finally jeopardizes its compliance with the GDPR. Accordingly, in those cases where the *Receiving Party* identifies such a conflict, the *Receiving Party* will not be entitled to process *personal data*. Where there is an adequacy decision by the European Commission, the assessment of the applicable law was already made. Nevertheless, it may be of interest of *the Parties* to sign these SDPC. In such a scenario, the performance of another assessment by each *Receiving Party* would be inappropriate. Nevertheless, the *Receiving Party* is obliged to regularly assess the validity of the adequacy decision and, in case such a decision is declared void, the *Receiving Party* shall be obliged to perform such an assessment.

(3) Where the *Receiving Party* becomes aware that a bilateral agreement (see Clause 3 (6)) becomes void, the *Receiving Party* shall notify the *Transferring Party*.	Although the *Transferring Party* has to ensure the existence of bilateral agreements, the *Receiving Party* shall be obliged to inform the *Transferring Party*, so that the *Transferring Party* is able to initiate appropriate steps (e.g. strong, encryption, splitting and spreading file segments). This also reflects the situation that the *Receiving Party* may have easier access to respective information and hence can provide such information to the *Transferring Party* already, where the *Transferring Party* have not been aware of it at all.
(4) The *Receiving Party* shall only process *personal data* on behalf of the *controller* and in compliance with the *Instructions*, these SDPC, the *Sub-Processing Agreement,* and the *Applicable Data Protection Law*.	The phrase "in accordance with the *Applicable Data Protection Law*" means, that the *Party* is obliged to process *personal data* in a way that enables the *controller* to comply with his obligations under the GDPR. This means, that the *processor* must ensure that his *processing* guarantees all the rights of the *data subject* under the GDPR, especially those according Chapter III of the GDPR (e.g. storing *personal data* only for a given purpose, being able to delete such data, respecting provisions related to automated decision making or *profiling*, etc.).
(5) The *Receiving Party* shall promptly and properly deal with all *Requests* of the *Transferring Party* relating to the *processing* of the *personal data* subject to these SDPC, the *Sub-Processing Agreement*, and the *Applicable Data Protection Law*.	Besides others, this includes the obligation corresponding to the right of the *Transferring Party*, Clause 2 (4)).
(6) The *Receiving Party* shall take reasonable steps to demonstrate to the *Transferring Party* upon reasonable *Written Request* that it implemented the technical and organizational measures according to its obligations under these SDPC, the *Sub-Processing Agreement*, and *Applicable Data Protection Law*.	Specific provisions of technical and organizational measures are expected in the *Data Processing Agreement* and/or *Sub-Processing Agreement*, and are therefore a matter which shall not be dealt with in detail in these SDPC. Therefore, technical and organizational measures include both, those being required by the *Sub-Processing Agreement* or the *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). However, if the *Data Processing Agreement* and/or *Sub-Processing Agreement* stays silent on technical and organisational measures, this provision shall ensure that appropriate measures will be implemented, as required by law.
(7) The *Receiving Party* shall notify the *Transferring Party* without undue delay in case:	The purpose of this provision is to secure the flow of information throughout the chain of *processors*. Notification duties do not create any obligation to actively investigate whether any of those circumstances apply. This is also reflected in different wording like "becomes aware" (positive fact of actually knowing), and "has reason to believe" (there are indications that raise concerns already, but there is actual knowledge yet). However, the *Receiving Party* must not refuse to become aware of circumstances either.
a) the *Receiving Party* has reason to believe that any *Instructions* by the *Transferring Party* conflict with these SDPC, the *Sub-Processing Agreement,* the *Data Processing Agreement* or the *Applicable Data Protection Law*;	Principally, the *Receiving Party* might only have reason to believe that *Instructions* conflict with the SDPC, the *Sub-Processing Agreement* or the *Applicable Data Protection Law.* However, the *Receiving Party* may also have reason to believe that *Instructions* conflict with the *Data Processing Agreement*, especially if the *controller* invokes its *third party* beneficiary rights.
b) the *Receiving Party* has reason to believe that any *Instructions* by the *Transferring Party* conflict with any legislation applicable to the *Receiving Party*;	
c) the *Receiving Party* receives contradicting *Instructions* by the *controller* and the *Transferring Party*; in such an event, the *Receiving Party* shall follow the latest *Instructions* received from the *controller*;	

d) the *Receiving Party* becomes aware of a *personal data breach* related to its *processing* of *personal data*;	*Personal data breach* here refers to the definition provided in Art. 4 (1) no. 12 GDPR.
e) the *Receiving Party* becomes aware of a circumstance which prevents or will prevent the *Receiving Party* to comply with these SDPC, *the Sub-Processing Agreement*, and the *Applicable Data Protection Law*, notably in the event of a change according to Clause 4 (2), (3) and (4);	
f) of a legally binding request of disclosure of the *personal data* processed by the *Receiving Party* by competent law enforcement authorities, unless otherwise legally prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.	
(8) Where the *Receiving Party* under the applicable law may be subject to requests of disclosure as set out by Clause 4 (7) f) that the *Receiving Party* must not communicate to the *Transferring Party*, either explicitly or aggregated, the *Receiving Party* shall inform the *Transferring Party* accordingly and provide information, under which circumstances this might appear in order to enable the *Transferring Party* to assess related data protection impacts.	The information must include whether or not the *Receiving Party* may be subject to the described requests of disclosure, and if yes, under which circumstances the respective data *processing* between the *Receiving Party* and the *Transferring Party* can be affected. This may include information about the respective law, court decisions etc.
(9) Where the *Receiving Party* becomes aware of a change in its applicable legislation or the application and interpretation thereof which is likely to have a substantial adverse effect on the warranties and obligations provided by these SDPC, the *Receiving Party* shall inform the *Transferring Party* accordingly and provide information, under which circumstances this might appear in order to enable	This obligation extends common provisions in this regard. Principally it is referred to change in the applicable legislation. Literally speaking, this only applies if there was a change in law, which leaves a gap in those scenarios where the law stays the same but its application due to a change in interpretation changed. However, it is not the mere legal text that defines an adequate level of data protection and safeguards the rights and freedoms of *data subjects*.

the *Transferring Party* to assess related data protection impacts.	It is the actual application of the law, and that is why this provision slightly extends the common phrasing.
(10) Where the *Receiving Party* engages any other *Sub-Processor* according to the *Sub-Processing Agreement* or *Data Processing Agreement:*	Because the *Receiving Party* poses a risk to the *Transferring Party* by engaging a further *Sub-Processor*, this provision governs the obligations regarding sub-*processing*.
a) the *Receiving Party* shall inform the *Transferring Party* about the engagement of a *Sub-Processor* and its related sub-*processing* according to the *Applicable Data Protection Law,* especially Art. 28 (2) GDPR;	
b) the *Receiving Party* shall sign SDPC with such *Sub-Processor* related to the *processing* of *personal data* under these SDPC, the *Sub-Processing Agreement*, the *Data Processing Agreement* and the *Applicable Data Protection Law*. The *Receiving Party* acknowledges and accepts that it is obliged to fulfil the same obligations of a *Transferring Party* as set out in these SDPC in the relation to any *Sub-Processor*. For avoidance of doubt: Any noncompliance of a *Receiving Party* with any obligation as of a *Transferring Party* in relation to any of its *Sub-Processors* results in a breach of contract of these SDPC in the relation to its *Transferring Party*;	This provision ensures that any *processor* within the processor chain is bound by these SDPC and therefore maintains the same level of protection for the *personal data*.
c) the *Receiving Party* shall make available upon *Request* to the *Transferring Party* a list of all *Sub-Processors* related to the *processing* of *personal data* under these SDPC or the *Sub-Processing Agreement*; the *Receiving Party* shall forward such *Request* to any applicable *Sub-Processors*, if there is no current list of *Sub-Processors* available. Any	The list of all *Sub-Processors* shall include the full name of the *Sub-Processor*, its legal entity, the country they are located in and where data will be processed, and the type of the sub-*processing* activity.

lack of completeness – e.g. if a *Sub-Processor* does not provide a list of *Sub-Processors* – shall be transparently communicated to the *Transferring Party*.	
d) the *Receiving Party* shall inform the *Transferring Party* about any changes to the *Sub-Processors* related to those *Sub-Processors* that are *processing personal data* under these SDPC, the *Sub-Processing Agreement;*	Changes relevant to these SDPC may be related to, e.g.: • location of corporate headquarters • location of *processing* activities • legal entity • merger and acquisitions
e) The *Receiving Party* shall immediately inform the *Transferring Party* if it was notified about or otherwise becomes aware of any *personal data breaches* of its *Sub-Processor* that affected the *processing* of the *Transferring Party's personal data*;	This obligation is only about the "forwarding" of a *data breach* notification the *Receiving Party* received itself by its *Sub-Processor*. Hence, no reasonable delay is expected and that is why the provision requires an immediate forwarding.
f) the *Receiving Party* shall instruct its *Sub-Processors* in accordance with the *Instructions* the *Receiving Party* received from the *Transferring Party* or from the *controller;*	
g) the *Receiving Party* shall – without undue delay – forward the *Requests* received from its *Transferring Party*, provided it relates to the *processing* of *personal data;*	
h) the *Receiving Party* shall immediately forward to the *Transferring Party* any information it has received from its *Sub-Processors* that materially impacts the *processing* of *personal data* under these SDPC, the *Sub-Processing Agreement* or the *Data Processing Agreement*; in case the *Receiving Party* determines the information is not materially	

relevant for the *Transferring Party,* the *Receiving Party* may refrain from forwarding the information. In this case, the *Receiving Party* has to document its reason for not forwarding the information;	
i) the *Transferring Party* is entitled to receive upon *Request* documentation related to the respective non-forwarding of the information according to h) once a year and whenever there is reason to believe that information has not been forwarded appropriately.	
(11) In case the *controller* invokes his *third party* beneficiary rights against the *Receiving Party*, the *Receiving Party* shall fulfil its obligations determined in this Clause to the *controller* as it would have fulfilled its obligations to the *Transferring Party*.	This provision ensures that the *controller*, in case he invokes his *third party* beneficiary rights, has the same rights as the *Transferring Party*. This includes, but is not limited, to give *Instructions* directly to the *Receiving Party*.
(12) In case the *Receiving Party* becomes aware that its *Transferring Party* or the *controller* has factually disappeared or has ceased to exist in law, unless any other legal entity has assumed the entire or relevant legal obligations of the *Transferring Party* or *controller* either by contract or by operation of law, as a result of which it takes on the rights and obligations of the *Transferring Party* or *controller*, the *Receiving Party* shall immediately terminate the *processing* of *personal data* of the respective *Transferring Party* or *controller* – including the deletion of such *personal data* -, unless otherwise provided by the *Sub-Processing Agreement*, *Data Processing Agreement* or *Applicable Data Protection Law*.	The *processing* of *personal data* by any *processor* is only justified insofar as the *processing* of the *controller* is justified. In the event that the *controller* disappears, this justification becomes void and the *processor* has no legal grounds to continue *processing* the respective *personal data*. The same applies to any *Receiving Party* in the event that its *Transferring Party* disappears. In that moment where the *Transferring Party* disappeared or has ceased to exist in law, there is still no contractual base to continue the *processing*. Notwithstanding the foregoing, the complexity of potential business models and business relationships may allow for specific contractual clauses within the *Data Processing Agreement* or *Sub-Processing Agreement* to foresee and plan for such an event. E.g. a *Sub-Processing Agreement* between a *Transferring Party* and a *Receiving Party* may provide that, in the event

	that the *Transferring Party* disappears, the *Receiving Party* shall cooperatively negotiate with the *controller* or any other precedent *Transferring Party* to take over the contractual relationship.
(13) Notwithstanding from Clause 4 (12) and in case the *Transferring Party* has factually disappeared or has ceased to exist in law, unless any other legal entity has assumed the entire or relevant legal obligations of the *controller* either by contract or by operation of law, as a result of which it takes on the rights and obligations of the *controller*, the *Receiving Party* shall inform the *controller* and act according to the *Instructions* of the *controller*; if the *Receiving Party* cannot determine the *controller* the *Receiving Party* shall delete the *personal data* concerned, unless otherwise provided by the *Sub-Processing Agreement*, *Data Processing Agreement* or *Applicable Data Protection Law*.	In case the *Transferring Party* has factually disappeared or has ceased to exist in law, the legal ground of *processing* still exists compared to the situation if the *controller* has factually disappeared or has ceased to exist in law. There may be practical needs to address this issue in the *Sub-Processing Agreement*. The SDPC do not want to limit necessary flexibility in this regard and hence accept solution as provided by *Sub-Processing Agreements*, as applicable.
(14) The Receiving Party shall designate in writing a *representative* in the EU according to Art. 27 GDPR.	The SDPC refer to a designated *representative* several times, mostly related to governing law and courts competent. It is expected that all *processors* will have such a *representative*. However, GDPR may lack applicability for very specific business models, which will result in a lack of competent courts in the EU. The latter is considered key under these SDPC as trust-enabler. To circumvent such a potential lack of applicability, this provision requires each *Receiving Party* to designate a *representative* as per Art. 27 GDPR.

Clause 5 Rights of the Receiving Party

(1) Upon reasonable *Written Request* by the *Receiving Party,* the *Transferring Party* shall provide information and documentation sufficient to demonstrate its com-	This provision ensures transparency and enforcement of the requirements that the *Transferring Party* must meet to engage a *Sub-Processor*. This includes having a signed *Data Pro-*

pliance with the applicable legal and contractual obligations for transferring *personal data* to the *Receiving Party*, especially those as under Clause 3 (2), (4) and (5).	*cessing Agreement* or *Sub-Processing Agreement* with its contractual partner and the authorization of the *controller* to engage another *processor* and to transfer *personal data* to a *Third Country*.
(2) Upon *Request*, the *Receiving Party* may assess relevant provisions of the *Sub-Processing Agreement* between its *Transferring Party* as a *Receiving Party* and the *Transferring Party*'s *Transferring Party*, i.e. the authorization of sub-*processing* and *Third Country* transfers, and regarding required technical organizational measures.	Additionally, to Clause 5 (1) this provisions clarifies that relevant provisions of the *Sub-Processing Agreements* must be disclosed.

Clause 6 Third party beneficiary rights

(1) There shall be *third party* beneficiary rights for the *controller* as follows:	
The Parties agree that the *controller* is a *third party* beneficiary of these SDPC and may act in his own name and on his own behalf. The *controller* is entitled	The following *third party* beneficiary rights shall enable the *controller* to exercise control over the *processing* to which he is entitled/obliged to do. Therefore, the SDPC grants rights to him that are equivalent to those set by the GDPR and the *Data Processing Agreement*. By that the *controller* can effectively asses a legal *processing* under GDPR without an unnecessarily administrative burden for *the Parties*.
a) to enforce against the *Receiving Party* Clause 4 (11); if the *controller* does so the *controller* demonstrates to the *Receiving Party* that the *controller* is the entitled *controller* and provides all information necessary for the *Receiving Party* to follow its *Instructions*;	This provision enables the *controller* to assume the role of the *Transferring Party*. More specifically, it gives the *controller* the same rights as the *Transferring Party* to enable it to act against the *Receiving Party* as necessary to enforce certain *Instructions*.

b) at its discretion to terminate any transfer and/or instruct the *Receiving Party* to delete, return, or suspend any *processing* of all *personal data* processed under these SDPC, the *Sub-Processing Agreement* and the *Data Processing Agreement* if	Even though the *controller* may not be a contractual partner of either *Party*, it must have the ability to terminate the transfer in certain circumstances to protect itself and the rights and freedoms of the *data subjects* concerned. This provision lays out the circumstances in which the *controller* has the right to terminate transfers to ensure the adequacy of the appropriate safeguards. Such circumstances may include the event that the *Receiving Party* has factually disappeared, ceased to exist in law, or has become insolvent. In any of these circumstances, the *controller* may directly enforce his rights.
1. the *Receiving Party* does not comply with its obligations to the *controller* according to Clause 4 (11) or	
2. the *controller* becomes aware of any circumstances according to Clause 4 (7) d), e), f) or (10) a), d) or e) regarding the *Receiving Party*.	
c) Notwithstanding Clause 6 (1) b) to request compliance of *processing* with the *Data Processing Agreement*, even if the *Sub-Processing Agreement* unlawfully conflicts the *Data Processing Agreement*.	
(2) There shall be *third party* beneficiary rights for *data subjects* as follows:	
a) *The Parties* agree, that any *data subject* is a *third party* beneficiary of these SDPC whose *personal data* are subject to the *processing* under these SDPC, the *Sub-Processing Agreement*. The *data subject* can enforce against the *Receiving Party* its rights under Chapter III of the GDPR, where	In accordance with the GDPR, these SDPC assume that the primary point of contact for the *data subject* will always be the *controller*. If the *controller* has factually disappeared or has ceased to exist in law, *data subjects* shall have the possibility to approach to any *processor* directly.

the *controller* has factually disappeared or has ceased to exist in law, unless any other legal entity has assumed the entire or relevant legal obligations of the *controller* either by contract or by operation of law, as a result of which it takes on the rights and obligations of the *controller*, provided the *Receiving Party* will be presented appropriate evidence that the respective *controller* has ceased to exist in law.	
b) *The Parties* do not object to a *data subject* being represented by a not-for-profit body, organisation or association according to Art. 80 (1) GDPR if the *data subject* so expressly wishes and if it is not prohibited by *Applicable Data Protection Law*.	It is essential for *the Parties* to agree on Clause 6 (2) b) since this is an explicitly stated right of the *data subject* according to Art. 80 GDPR.

Clause 7 Infringement of the obligations

(1) The *Transferring Party* shall immediately and thoroughly terminate the transfer in case the *Receiving Party* does not comply with Clause 4 (2), does not fulfil the obligations according to Clause 4 (3), (4), (6), (7), (10) or (11) or has complained without justification about competence of the court according to Clause 10 (1) lit. a) and shall accordingly instruct the deletion or return and deletion of any *personal data* processed under these SDPC, the *Sub-Processing Agreement* or *Data Processing Agreement* by the *Receiving Party*.	An infringement of the obligations implies a lack of protection of *personal data*. Hence, it is mandatory to terminate the transfer immediately in such circumstances because the rights and freedoms of the *data subject* might be at risk. Clause 7(1) provides an obligation for the *Transferring Party* to terminate the transfer in the circumstances described herein. Notwithstanding the foregoing, Clause 7(2).provides an exception to this general obligation.
(2) Notwithstanding from Para (1) the *Transferring Party* may at its discretion suspend the transfer, request deletion and/or request the return of the *personal data*. This might be the case where the *Transferring Party* needs appropriate time to manage the porting of respective *personal data* to another *processor* or the *Receiving Party* substantially promises to re-establish its technical	There may be circumstances where a final termination of the transfer seems excessive. This provision gives an example of such circumstances and provides an opportunity for the *Receiving Party* to renew its compliance with its obligations under the SDPC. The *Transferring Party* thus retains the possibility to keep its engagement with this *Sub-Processor*.

and organizational compliance with these SDPC or provide requested information by the *Transferring Party* in a timely manner. The *Transferring Party* shall document its reasons why such a suspension was considered appropriate. After a maximum of three months any suspension shall be considered inappropriately with regards to the re-establishment of the technical and organizational compliance. It shall also be considered inappropriate with regards to the provision of any information according Clause 4 (5) and (6) requested by the *Transferring Party* unless the *Receiving Party* demonstrates that its delayed provision is caused by circumstances that the *Receiving Party* has no direct influence on the delay but can demonstrate it has taken all necessary measures to receive the information in a timely manner itself.

Another circumstance may be where the *Receiving Party* has a justifiable reason for not complying with the *Requests* of the *Transferring Party*. This provision provides an exception for those circumstances where a final termination of the relationship between *the Parties* may seem inappropriate.

Such a grace period is also protecting the rights and freedoms of *data subjects*. Any ad-hoc termination of transfer will most likely trigger the need for an ad-hoc replacement, requiring to transfer *personal data* from one *processor* to another, who needs to be appropriately assessed by the *Transferring Party* prior to any *processing*. It is obvious that such a burdensome procedure should not be triggered by any infringement, but only to those that are substantial.

Clause 8 Liability

(1) Any *data subject* who has suffered legally cognizable damage as a result of an infringement of these SDPC and the *Sub-Processing Agreement* or *Data Processing Agreement* may request compensation from any *Party* of these SDPC for the damage suffered, in accordance with Art. 82 GDPR.

The specification of indemnities in Clause 8 follows Art. 82 GDPR. Clause 8 (1) determines the external liability of *the Parties* towards the *data subject*, which is essential for full and effective compensation. According to Art. 82 (2) GDPR, this contract provides that the *Initial Processor* and any *Sub-Processors* may be held directly liable for damages resulting from *processing* that is in breach of the obligations set out in GDPR.

This only applies to external liabilities against *data subjects*. It does not affect any internal liabilities agreed upon by *the Parties*.

(2) *The Parties* shall be jointly and severally liable to the *controller* for any damages the controller has suffered as a result of any breach of the obligations of these SDPC, the *Sub-Processing Agreement*, the *Data Pro-*

Clause 8 (2) determines *the Parties'* liability towards the *controller* within the processing chain. Such liability is based on an extensive interpretation of Art. 82 GDPR in conjunction with Art. 28 (4) Sentence 2 GDPR. Both *Parties* are jointly and severally liable, with the possibility of an internal settlement where compensation may be

cessing Agreement or *Applicable Data Protection Law* by *the Parties* and any further *Sub-Processors*.	appointed according responsibility. This issue falls outside the scope of the SDPC and shall be determined in the *Sub-Processing Agreement* between *the Parties*.
(3) Para. (1) is without prejudice to the liability of the *controller* according to the *Data Processing Agreement* and *Applicable Data Protection Law*.	Clause 8 (3) provides the separation of the initial *controller*'s liability. Because the *controller* is not a direct contracting *Party* to these SDPC, this shall be part of the *Data Processing Agreement* with the *controller*.

Clause 9 Cooperation with supervisory authorities

The Parties agree that the competent *supervisory authority* may perform its rights according to Art. 58 GDPR against each of them, to the extent it concerns the *processing* covered by these SDPC.	This Clause refers to Art. 58 GDPR. Hence, the *supervisory authority* has the same rights in a *Third Country* as in the EU. This ensures that the *data subject* is also protected by an independent body.

Clause 10 Dispute Resolution Mechanism

(1) *The Parties* acknowledge and agree that with regards to any disputes with the *data subject* the following applies:	This Clause regulates the possibilities of disputes between *data subjects* and *the Parties*.
a) The *Receiving Party* guarantees that it does not challenge or object to the competency or jurisdiction, where any *data subject* brings procedures related to the *processing* of its *personal data* under these SDPC to a court where either the *controller* or the *Receiving Party* is established, where the *controller* or the *Receiving Party* has registered its *representative* according to Art. 27 GDPR or where the *data subject* has its habitual residence. The *data subject* may explicitly refer to this provision where the *Receiving Party* complains about the competence of the court.	Art. 79 (2) GDPR grants *data subjects* very specific rights as regards in which courts *data subjects* may bring proceedings. International procedural law, however, will not grant *data subjects* the same options. Art. 79 (2) GDPR provides that *data subjects* may bring proceedings in those courts situated where • the *controller* or *processor* has an establishment; or • the *data subject* has his or her habitual residence In both cases, the GDPR takes it for granted that the courts will be situated in a member state.

	Considering international transfers, there are two challenges: • how to address a *controller's* or *processor's* representative according to Art. 27 GDPR; and • how to address that *processor*s may not have their establishment in any member state The mere existence of the necessity for further safeguards in international transfers proves that the legislature did not provide for every circumstance where the GDPR should be applicable to *processor*s. Hence, *data subject*s would suffer negative effects without an SDPC reflecting the spirit and purpose of Art. 79 GDPR.
b) The *data subject* may refer its complaint to alternative dispute resolution mechanisms, like mediation by an independent person or, where applicable, by the competent data protection *supervisory authority* according to the *Applicable Data Protection Law*, as provided in this section. If a *Party* has declared itself subject to an alternative dispute resolution mechanism, the *data subject* shall refer its dispute to this respective alternative dispute resolution mechanism. If a *Party* has not declared itself subject to an alternative dispute resolution mechanism the *data subject* shall communicate to the *Party* concerned that it is willing to refer the dispute to an alternative dispute resolution mechanism and to which. The *Party* concerned shall promptly respond whether it will declare itself subject to this alternative dispute resolution mechanism. If the *Party* concerned rejects the alternative dispute resolution mechanism proposed by the	Lit. b) offers the *data subject* the possibility to look for a mediation before going to court. This grants the *data subject* more extrajudicial possibilities. This reduces the organizational burden for the *data subject* and offers a chance to relieve the courts and bring an opportunity to both sides the *data subject* and the accused *Party*. But this decision shall be up on the choice of the *data subject*. It is entitled to directly go to court without taking this chance.

data subject the *data subject* shall refer to the competent court. For avoidance of doubt: - *Data subject's* choice to refer any dispute to an alternative dispute resolution mechanism does not prevent the *data subject* to refer such dispute to court if any such mechanism has failed; - A *data subject* should not refer the same dispute between the *Party* concerned and the *data subject* to court proceedings and alternative dispute resolution mechanisms at the same time; - Court proceedings do not require the *data subject* to have been defeated within any prior alternative dispute resolution on the same dispute.	
(2) *The Parties* acknowledge and agree that with regards to any disputes between *the Parties* the court competent is the one where the *Transferring Party* is established. Where the *Transferring Party* is not established within the EU, the court competent shall be the one where the *representative* of the *Transferring Party is* established.	The purpose of Clause 10 (2) is to determine which court shall be exclusively competent regarding disputes between *the Parties*. Hence it does not affect the court competent for disputes between the *controller* and one of *the Parties* or between the *data subject* and one of *the Parties*. For disputes related to any *data subject* this is reflected in Clause 10 (1) a) and b). For disputes related to the *controller* no provisions were necessary, as International Civil Procedure Law already provides adequate safeguards. Considering the fact, that the current model clauses for the transfer of *personal data* to *processors* (Commission decision 2010/87/EU) also refer the disputes to the courts of the member state were the "data exporter" is established (see Clause 9 Standard Contractual Clauses (Processors)) it was decided within the SDPC to refer the disputes to the courts of the member state were the *Transferring Party* is established and in case the *Transferring Party* is not established within the EU, in the member state where

	the *representative* of the *Transferring Party* is established. This option was chosen since it provides legal certainty and continuity. The link to the EU ensures an adequate application of the GDPR by interpreting these SDPC.
(3) *The Parties* may agree to a court competent at their choice, provided that such court competent is one within the EU.	It shall be guaranteed that the court competent is a court within the EU in order to safeguard an appropriate application of the GDPR.
(4) *The Parties* may agree to refer the dispute to mediation by the *supervisory authority* competent where applicable according to the *Applicable Data Protection Law*.	

Clause 11 Governing Law

(1) Governing law regarding any dispute related to these SDPC claimed by the *data subject* against a *processor* according Clause 6 (2) shall be the law of the member state where the *data subject* has its residence; in case the *data subject* is a non-EU resident the law of the state where the *data subject* has its residence shall apply, unless the *data subject* requests the law of the member state where *the processor* has registered its EU *representative*.	Since the *data subject* will have usually less possibilities to overview which parties are involved and where *the Parties* are established, it is necessary that the *data subject* does not have difficulties regarding governing law. In case of a claim, it should not deal with a governing law which it does not know. In order to avoid complexity, *the Parties* should agree upon the governing law of the state where the chosen place of jurisdiction is.
(2) As the governing law regarding any dispute related to these SDPC between *the Parties*, *the Parties* acknowledge and accept the law of the following member state of the EU_____. *The Parties* acknowledge and agree in case the dispute resulted of these SDPC affects rules of the *Sub-Processing Agreement* or	The *Parties* are free to express their choice of governing law with the limitation that it shall be the law of one of the member states of the EU (Art. 28 (4) GDPR).

Data Processing Agreement between the *Parties* the governing law of these SDPC has precedence.	
(3) In case the *controller* invokes his right according Clause 6 (1) the governing law referred to in Para. (2) of this Clause shall apply.	In order to have the same governing law for disputes from the *controller* towards a *Party* as between *the Parties* Para. (3) refers to Para. (2).

Clause 12 Implementation of a suspensive condition

(1) These SDPC shall only become effective under the suspensive condition that the following appropriate safeguards according Art. 46 (2) GDPR becomes ineffective, namely cases where the Commission has decided that the *Third Country* ensures an adequate level of protection according to Art. 45 (1) GDPR. Where the transfer of *personal data* under these SDPC is also subject to an approved Code of Conduct, the provisions of the respective Code of Conduct shall prevail.	The SDPC shall provide an adequate level of protection for the transfer of *personal data* into or within a *Third Country*, especially in those circumstances where the Commission has not made a decision on the matter according to Art. 45 GDPR. Moreover, these SDPCs shall enable the *processor*s who use them as a safeguard in circumstances where the decision of the Commission is repealed to amend or suspend the data transfer according to Art. 45 (5) GDPR.
(2) ☐ Notwithstanding from Clause 12 (1) *the Parties* agree, that these SPDC shall only become effective under the suspensive condition that the following appropriate safeguards become ineffective: ☐ adequacy decision of the European Commission, Art. 45 (1) GDPR ☐ an approved Code of Conduct, Art. 46. (2) (e) ☐ an approved certification mechanism, Art. 46. (2) (f) ☐ binding corporate rules, Art. 46. (2) (b) ☐ there shall not be any suspensive condition.	This provision can be optionally selected by *the Parties* as an alternative to Clause 12 (1). There may be cases, where *the Parties* even prefer to have the SDPC applicable instead of having any suspensive condition at all. For this purpose, *Parties* may now choose to either take the static provision as provided by the SDPC or to agree upon a more dynamic provision where *the Parties* select the respective suspensive conditions individually. Remark: in cases, where there shall be no suspensive condition the respective *Parties* must ensure that all the provisions flowed down do not create any conflicts.

Clause 13 Variation of contract

(1) These SDPC must not be modified or otherwise be amended by *the Parties*. This does not preclude *the Parties* from adding clauses on business related issues which they consider as being pertinent for the contract as long as they do not directly or indirectly contradict or otherwise undermine the rights and obligations as set out in these Clauses. In case of conflict, these SDPC precedent over any contrary clauses.	To guarantee the full level of protection for *personal data*, *the Parties* are not allowed to amend these Clauses unless they add clauses which do not contradict the content of these SDPC. Different *processing* activities and business models may require additional business-related provisions which enable them to fulfil their contract. The SDPC shall provide a framework which is useful for these different business models.
(2) Para. (1) does not preclude *the Parties* from expanding upon these Clauses in further agreement as long as the safeguards of these SDPC are warranted.	Compared to Para. (1), this provision allows *the Parties* to add safeguards that do not fall below the level of data protection as provided by the SDPCs. This may be the case where a member state requires a higher standard of data protection or where *controllers* contractually require additional safeguards.
(3) Where *the Parties* have signed a *Sub-Processing Agreement* or a *Data Processing Agreement* without obligation under GDPR – e.g. where *Receiving Party* is considered to perform services that are not principally related to the *processing* of *personal data*, for instance specific types of maintenance services – and hence these SDPC are signed to safeguard *Third Country* transfers of data under such an precautionary executed agreement, i.e. there is no legal obligation under GDPR to sign those SDPC as well, *the Parties* may modify and adversely derogate these SDPC with regards to the following provisions: Clause 2 (4), Clause 3 (4),(5), (7) a), b), Clause 4 (5), (10) b) (but no derogation that is less protective than Article. 11 para 2 GDPR), c), f) (11) (but no derogation that is less protective than Article. 11 para 2 GDPR), Clause 5, Clause 6 (2), Clause 8 and Clause 9.	Regarding the feedback received there is a practical need of signing *Sub-Processing Agreements* or *Data Processing Agreements* and SDPC even in those cases, where this is not mandatory by law. It is not recommended using the SDPC to solve data protection related issues that are not directly related to *Third Country* transfers. However, given the practice of signing SDPC as an additional safeguard without legal obligation, the current draft should not hinder this positive practice in future. Instead of drafting this provision against the background of one specific issue, the approach was to find a solution that will work for the specific scenario reported (maintenance) but also any scenarios that are of a similar kind. This provision balances both the interest and intent of SDPC to safeguard international transfer and the interest of a flexibility with regards to unnecessary administrative burdens for signees.

The current proposal follows the approach that the SDPC do not govern specific technical or organizational measures related to the *processing* of *personal data* in general. Where *the Parties* consider it necessary, however, to balance such derogations from administrative burdens with intensified provisions regarding limitation of *processing* purposes or any other technical and organizational measures – e.g. related to the deletion of received *personal data* or clarify the applicability of Article 28 para 10 GDPR – those provisions shall be subject to the individual *Sub-Processing Agreement* or *Data Processing Agreement* but not the SDPC.

Clause 14 Termination of contract

Any *Party* may terminate these SDPC any time with prior *Written* notification of one month.

The SDPC contain a regular right to terminate them whereas the draft of the ad hoc Clauses of the WP29 stipulated an obligation for the *Transferring Party* to terminate the Model Clauses in certain circumstances. Comparatively, this draft refrains from setting an obligation of termination of contract because a *Party* should have the right to terminate a contract rather than an obligation.

An obligation to terminate the transfer in order to maintain the protection of *personal data* must be provided, though. This provision is set out in Clause 15 of these SDPC.

Clause 15 Termination of the transfer and instruction of deletion or return and deletion

(1) The *Transferring Party* shall immediately terminate any transfer and instructs the deletion or return and deletion of any *personal data* subject to these SDPC by the *Receiving Party* in case of and where not explicitly provided differently in these SDPC:

Solely terminating the SDPC or the *Sub-Processing Agreement* would not guarantee the appropriate level of protection of *personal data* in those circumstances where it is required that the transfer will be stopped immediately. Those cases are addressed in this Clause.

a) the *Data Processing Agreement* has been terminated;	In the event of the termination of the *Data Processing Agreement*, the legal ground for sub-*processing* according to Art. 28 GDPR ceases to apply. Any further transfer of *personal data* must be prevented.
b) the *Sub-Processing Agreement* has been terminated;	As in the circumstance described above, the legal ground for *Sub-Processing* according to Art. 28 GDPR ceases to apply when there is a termination of the *Sub-Processing Agreement*.
c) these SDPC are terminated according to Clause 14 and the transfer of *personal data* is not subject to any other safeguard according Chapter V GDPR;	The normal use case of termination of the transfer is the regular termination of the SDPC.
d) the *Transferring Party* becomes aware of any infringements of these SDPC, the *Data Processing Agreement*, the *Sub-Processing Agreement* or *Applicable Data Protection Law;* where Clause 7 applies Clause 7 shall prevail.	Clause 7 SDPC provides an additional Clause regarding infringements because of its importance. It rules the details of infringements and provides a case where the transfer can be terminated temporarily; that differs this regulation from the others within this Clause.
(2) The *Transferring Party* shall request *Written* confirmation, and where appropriate any further demonstration, by the *Receiving Party* to have	In order to ensure the transfer is terminated it is necessary for the *Transferring Party* to require the *Documented* termination of the data transfer by the *Receiving Party.*
a) terminated any transfer and instructed deletion or return and deletion of any *personal data* subject to these SDPC by any *Sub-Processor*, where applicable	
b) deleted or returned and deleted any *personal data* subject to these SDPC.	

On behalf of the Provider

Name (written out in full): ...

Position: ...

Address: ...

Other information necessary in order for the contract to be binding (if any): ...

(Stamp of organization) Signature: ...

On behalf of the Customer

Name (written out in full): ...

Position: ...

Address: ...

Other information necessary in order for the contract to be binding (if any): ...

(Stamp of organization) Signature: ...