Feedback from NLdigital on the European Commission's Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries (ref. Ares(2020)6654686 - 12/11/2020)

Place: Breukelen, the Netherlands
Date: December 10, 2020

NLdigital is the trade association for ICT and telecom companies in the Netherlands. NLdigital represents the industry's interests in dealing with the government and political world. More than 650 ICT companies in the Netherlands are members. Our members range from multinationals to SMEs, from all segments of the industry, making us the foremost advocate and representative of the Dutch digital sector. About eighty percent of our members are small- and medium-sized enterprises (SMEs). The majority of our members process personal data on behalf of their clients as part of their core business and are therefore data processors under the GDPR.

We have developed the 'Data Pro Code', the first (and so far the only) approved Code of Conduct under the GDPR by the Dutch Data Protection Authority (the Dutch DPA). The Data Pro Code is especially designed for SMEs in their role as processor. We all know the discussions and concerns people have surrounding big tech companies, but we should not forget that a large part of processing is performed by SMEs established within the EU. An important addition to the Data Pro Code is a neutral processing agreement, which covers both the responsibilities of the controller and the processor. Large companies can afford to hire lawyers that can draft contracts that comply with the GDPR in detail. Smaller companies do not always have these means. Therefore our Data Pro Code processing agreement is drawn up for them, impartially, so it can be used for the relationship controller – processor but also for the relationship processor – sub processor. A standard processing agreement should fulfil the needs of SMEs as much as, or even more than, the bigger companies. That is why we advocate that the SCCs that are published by the European Commission should also be a tool for smaller companies with which to comply with the GDPR.

We are happy to have the opportunity to provide input on the draft SCCs and we can see the Commission has put a lot of effort into this. The Schrems II ruling has put a great burden on the shoulders of multinationals and SMEs of our industry. We believe that a risk based approach is the way to go forward in order to have transfer mechanisms that are sustainable. However, we feel it is mostly a political problem, that needs a transatlantic political solution. We urge all parties involved to work out a solution as soon as possible. Still, we have some remarks that we would like to point out. We are happy to be able to provide suggestions. In order to ensure that the SCCs will be viable for SMEs, we call for the SCCs to provide workable clauses that will allow for businesses and organisations to adopt measures to ensure that they can continue to transfer data in a manner which respects the essence of EU data subjects' GDPR rights without detracting from other Charter rights of EU organisations. The general remarks are elaborated on here below. The in-depth comments can be found in **Annex I**.

1. Maintaining a risk based approach

We endorse that the SCCs retain the risk based approach to international transfers. This takes into account the factual circumstances and individual context of data transfers that need to be assessed based on associated risks on the ground and in practice. This is consistent with the GDPR and rulings of the CJEU. We urge the European

Commission to retain and integrate this approach in the final version. This can be assisted by including references to the accountability principle of the GDPR. The risk based approach is important as it prevents unrealistic or misleading expectations being placed on organisations for factors outside their control.

Comparatively, the draft EDPB recommendations run counter to the GDPR's risk based approach, the CJEU ruling itself and these draft SCCs. Harmonisation between the GDPR, SCCs and EDPB recommendations in favour of a risk based approach is desired.

2. One-year transition period

Organisations are given a one-year transition period to implement the SCCs. Provided the significant challenges many organisations will face in adopting these SCCs, especially regarding safeguards and measures for data transfers to third countries, this transition period is too short. We would suggest to implement a transition period of two years.

3. Means and capability

The clauses are drafted under the assumption that companies will have enough capability to abide by these clauses. In particular, the obligation to take into account the specific circumstances of the transfer, the laws of the third country of destination relevant in light of the circumstances of the transfer and any additional safeguards (including technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination), places a heavy burden on SMEs. It would – for example - require a highly complex assessment requiring specialist multi-jurisdictional legal and technical advice, to be routinely re-evaluated, which many businesses, especially SMEs, won't have available and/or can't afford. This curtails innovation for EU SMEs and leads to unfair competition.

Furthermore, there is no need to replicate / duplicate the existing article 28 obligations in Module 2 and Module 3, as the purpose of the new SCCs is simply to address specific issues arising from transfers to third countries. Many organisations have invested in drawing up data processing agreements according to Article 28(3) of the GDPR. Clause 4 ('Hierarchy') states that the SCCs shall prevail in the event of a conflict with any other agreement. If companies want to address transfers to third countries via these SCCs, their time, energy and means invested in their previous tailor-made processing agreements should not be substituted for these standard clauses that do not always fit specific circumstances. Companies should be able to combine their existing processing agreements with the clauses in the SCCs regarding data transfers to third countries, in which the SCCs would be supplemental.

4. Confusing format

First of all, the EDPB Guidelines 07/2020 on the concepts of controller and processor state (nr. 102) that 'the processing agreement should not merely restate the provisions of the GDPR'. However, the clauses in the consulted document do restate quite a few texts from the GDPR (although not word-for-word, but in quite similar wording). The substantive shaping of clauses therefore needs to occur in the annexes of the document. In practice, this means that the emphasis should be on these annexes. It is therefore recommendable to start the document with the subject matter (now set out in the annexes), which should then be followed by the standard

clauses. This way, it can be ensured that the completion of the subject matter receives the necessary attention and scrutiny from the parties.

5. Relationship sub-processor and controllers / data subjects

When using Module 3 (processor to processor, P2P), it is unworkable to require controllers to be parties to the SCCs in the event of digital supply chains where customers (acting as processors) may have a great amount of end users (acting as controllers) and data subjects who are unknown to the sub-processor. Module 3 imposes direct obligations on the sub-processor to cooperate with, and notify controllers and data subjects in specific circumstances. Given the creation of third party beneficiary rights for data controllers to enforce the SCCs against sub-processors, and the existing rights for data subjects under GDPR to enforce rights against sub-processors, sub-processors should not have to interact with controllers or data subjects in P2P transfers. This leads to practical obstacles, and doing so potentially creates tension with contractual commitments and confidentiality obligations between the sub-processor and the data exporter.

Our more detailed comments on specific articles can be found in **Annex I**.

Kind regards,

Lotte de Bruijn
Managing Director

Annex I

Remark no.	*Where*	*Section*	*Module*	*Clause*	*Sub*	*Original text*	*Remark*
1	**In general**					.	Begin the document with the subject matter and make this more flexible.
2	**Annex**	**2**	**2, 3, 4**	**1.1**	**a**	[…] The data importer shall process the personal data only on documented instructions from the data exporter. […]	This implies that every controller will specify its own instructions. This does not work in practice for a standard product. **Proposed change:** *'Processor shall not process personal information for any other purpose then laid down in this processor agreement.'* Parties can then agree on a standard text in annex I.B where processor can explain how his standard service processes the data from controller. It is up to controller to decide whether the service serves his needs and is sufficient to comply with the GDPR.
3	**Annex**	**2**	**2, 3**	**1.2**		The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in	With this wording, the obligation of purpose limitation is wrongfully imposed on the processor. 'Specific purposes' is too far-reaching.

						Annex I.B [Description of the transfer(s)].	**Change proposed:** *'The data processor shall process the personal data on behalf of the data controller, in accordance with the written instructions provided by the data controller and accepted by the data processor, as set out in Annex I.B.'*
4	**Annex**	**2**	**2**	**1.3**		The Parties shall provide the data subject with a copy of the Clauses upon request. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II, the Parties may redact the text of the Annexes to these Clauses prior to sharing a copy, but shall provide a meaningful summary where otherwise the data subject would not be able to understand the content of the Annexes. This is notwithstanding the obligations of the data exporter under Articles 13 and 14 Regulation (EU) 2016/679, in particular to inform the data subject about the transfer of special categories of data.	According to the GDPR (Article 12), the controller has this obligation. This would need to be harmonised with the GDPR.
5	**Annex**	**2**	**Module 1: clause 1.5**			The Parties shall implement appropriate technical and organisational measures to ensure the security of	**Remark 1:** Here, a reference to codes of conduct and certifications that guarantee an appropriate level of

			Module 2: clause 1.6 **Module 3: clause 1.6** **Module 4: clause 1.2**		the data, including during the transmission, and the protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. In assessing the appropriate level of security, they shall take due account of the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing […]	adopted measures should be included. The arrangement regarding technical and organisational measures is a key component in a processing agreement. As such, it is preferable that there is a separate clause on technical and organisational measures, to emphasize the importance. Also, it is preferable to add the following sentence: '*Data processor does not guarantee that its security measures shall be effective under all circumstances.'* **Remark 2:** The wording 'they … take due account' (wrongfully) imposes an obligation for the processor. Preferably, replace 'they' with 'controller'. The processor needs to inform the controller very clearly in the annexes about the specifics of their service, for what use it is suited, and what their adopted (security) measures are. And, if necessary, the controller needs to ask for further required information. The controller can then make an informed decision whether the level of security of the processing will be appropriate and if he can employ the processor for

						his intended purpose of processing. Also, it is not clear how it works in practice when parties have assessed that additional measures need to be implemented (see also general remark 2 regarding flexibility and the possibility of adjusting to changing circumstances). **Addition proposed:** *'Data processor shall be entitled to adjust the security measures it has implemented if to its discretion such is necessary for a continued provision of an appropriate level of security.'* Also, a chart can be added in Annex VII, which includes the minimum elements that the processor needs to inform the controller about. Furthermore, when providing a standard software service to multiple controllers, processors can not always meet every request from different controllers. **Addition proposed:** '*Controller may request data processor to implement further*

							security measures. Data processor shall not be obliged to honour such requests to adjust its security measures. If data processor makes any adjustments to its security measures at the data controller's request, data processor is entitled to invoice controller for the costs associated with said adjustments. Data processor shall not be required to actually implement the requested security measures until both parties have agreed upon them in writing.'
6	**Annex**	**2**	**2**	**1.5**		Processing by the data importer shall only take place for the duration specified in Annex I.B. Upon termination of the provision of the processing services, the data importer shall [[OPTION 1] delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so / [OPTION 2] return to the data exporter all personal data processed on its behalf and delete existing copies]. This is notwithstanding any requirements under local law applicable to the data importer prohibiting return or destruction of the personal data. In that case, the data importer [warrants] that it will	**Remark 1:** Parties should be able to continue to make the choice whether to delete or return transferred data at the end of the provision of the services, rather than at the outset. **Change proposed:** '*If the data processing agreement is terminated, data processor shall delete all personal data it currently stores and which it has obtained from controller within the timeframe laid down in the processing agreement, in such a way that the personal data can no longer be used and shall have been rendered inaccessible. Alternatively, if such has been agreed, data processor shall return the personal data to controller in a machine-readable format.'*

						guarantee, to the extent possible, the level of protection required by these Clauses and will only process it to the extent and for as long as required under that local law.	**Remark 2:** This should take into account the potential costs for the processor of erasure or return of data. **Addition proposed:** *'If data processor incurs any costs associated with the provisions of this article 1.5, it shall be entitled to invoice data controller for said costs. Further arrangements relating to this subject can be laid down in the contract.'*
7	**Annex**	**2**	**Module 1: clause 1.5** **Module 2: clause 1.6**		**(b)**	The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.	**Addition proposed:** *'Data processor shall be entitled to provide third parties with personal data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.'* *'Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by data processor to data controller, and any and all information provided by data processor to data controller detailing the technical and organisational security measures included in the contract are confidential and shall be treated as such by data controller and shall only be disclosed to authorised employees of data controller. Data controller shall ensure that its*

							employees comply with the requirements described in this article.'
8	**Annex**	**2**	**3**	**1.6**	**(c)**	In the event of a personal data breach concerning personal data processed by the data importer, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate, the controller after having become aware of it. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided subsequently as it becomes available without undue delay.	The data importer may not always know wo the controller is.
9	**Annex**	**2**	**2, 3**	**1.6**	**(d)**	The data importer shall cooperate in good faith with and assist the data exporter in any way necessary to enable the data exporter to comply with its obligations under	Notifying the DPA remains an obligation for the controller, and should not be passed on to the processor. This division in obligations should remain clear. 'To assist in any way necessary' is too wide a scope. The assistance

						the GDPR, notably to notify its controller so that the latter may notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.	given should be restricted to 'reasonable assistance'. Also, this clause should take into account the potential costs for the processor. **Addition proposed:** *'If data processor incurs any reasonable costs in doing so, it is entitled invoice data controller for these, at the rates applicable at the time.'*
10	**Annex**	**2**	**2, 3**	**1.7**		To the extent the transfer includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "special categories of data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may for instance include restricting personnel permitted to access the personal data, additional	In this wording, the obligations of the controller are imposed on the processor, again. The controller needs to assess if the services the processor provides are appropriate for the processing of special categories of data. And if so, the controller needs to specifically inform processor if he wants to process any special categories of data and instruct the data processor to apply specific instructions in the annexes. **Change proposed:** *'Unless explicitly stated otherwise in the contract, the products and services provided by data processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.'*

						security measures (such as pseudonymisation) or additional restrictions with respect to further disclosure.	
11	**Annex**	2	3	1.9	(c)	The data importer shall make available to the data exporter and the controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and allow for and contribute to reviews of data files and documentation, or to audits of the processing activities covered by these Clauses, in particular if there are indications of non-compliance. In deciding on a review or audit, the controller or data exporter may take into account relevant certifications held by the data importer.	First remark for this article: It is unrealistic for the data importer to permit and/or be required to be audited by the data exporter, as well as the controller Second remark: **Change proposed** The data importer shall make available to the data exporter and the controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and allow for and contribute to reviews of data files and documentation~~, or to.~~ Audits of the processing activities covered by these Clauses are only allowed if there are indications of non-compliance and there is no ~~relevant . In deciding on a review or audit, the controller or data exporter may take into account relevant~~ certification~~s~~ held by the data importer. Third remark: The requirements of the auditor need to be emphasised and the grounds for auditing need to be limited in order to strike a fair balance between the interests of the controller and the processor. **Addition proposed:** *'At data controllers request, data processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing*

							agreement. If, in spite of the foregoing, data controller has grounds to believe that the personal data are not processed in accordance with the data processing agreement, data controller shall be entitled to have an audit performed (at its own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the processing agreement. The scope of the audit shall be limited to verifying that data processor is complying with the arrangements made regarding the processing of the personal data as set forth in the present data processing agreement.'
12	**Annex**	2	2, 3	1.9	(e)	The data importer shall make the information referred to in paragraphs b) and c), including the results of any audits, available to the competent supervisory authority on request.	Results of audits can contain security vulnerabilities which should, in order to protect data subjects, preferably remain confidential. Furthermore, DPA's already have the opportunity to request any information necessary under the GDPR, so this does not need to be reiterated here. **Change proposed:** *'The auditor or expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify data controller of matters which cause data processor to fail to comply with its obligations under the data processing agreement. The expert shall furnish data processor with a copy of his/her report.'*

							Also, the clauses do not specify what needs to be done with the results of de audit. **Addition proposed:** '*The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data processor shall implement the proposed measures for improvement insofar as to its discretion such are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.'* *'Data processor shall be entitled to invoice data controller for any costs it incurs in implementing the measures referred to in this article.'*
13	**Annex**	**2**	**1, 2, 3, 4**	**2**	**(b), (c), (d)**	The Parties warrant that they have no reason to believe that the laws in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from	It would require a highly complex assessment requiring specialist multi-jurisdictional legal advice, to be routinely re-evaluated, which many businesses will not have available to afford. In addition, the cost of implementing this would make many businesses unviable or prohibitively onerous.

						fulfilling its obligations under these Clauses. This is based on the understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses.	
14	**Annex**	**2**	**1, 2, 3, 4**	3.1	(a) i, (a) ii	The data importer agrees to promptly notify the data exporter and, where possible, the data subject (if necessary with the help of the data exporter) if it: (i) receives a legally binding request by a public authority under the laws of the country of destination for disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; EN 15 EN (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include	The Commission might consider to provide the opportunity to deviate from informing the data subject on such short notice if that's necessary for public reasons such as emergency reasons or public safety. Also the data importer might not know the data subject, so that informing the company that has a direct relation with the controller, might suffice.

						all information available to the importer.	
15	**Annex**	**2**	**1, 2, 3, 4**	3.2		The data importer agrees to review, under the laws of the country of destination, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the data importer pursuant to Clause 2(e) of this Section. (b) The data importer agrees to document its legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make it available to the data exporter. It shall also make it available to the competent supervisory authority upon request.	Same explanation as above under remark 6.
16	**Annex**	**2**	**2, 3**	**4**	**(a)**	[OPTION 1] The data importer shall not	The sequencing is incorrect. The data importer cannot engage prior

						subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without its prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date. OPTION 2 GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s). The list of sub-processors the data importer intends to engage can be found in Annex III. The data importer shall inform the data exporter in writing of any intended changes of that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The Parties shall keep Annex III up to date.	to the agreement of the data exporter. Option 2 is less restrictive than option 1, but still too narrow due to the obligation to inform the controller of 'any intended changes in advance', at least at a specified time period in advance. In practice, flexibility in employing different sub-processors is needed to be able to adjust to changing circumstances. One way of doing this is that the processor publishes a list of employed sub-processors at their website, for example with entity name, service provided and location (country) of the sub-processor, and report any change in this list. **Change proposed:** *'Data processor has specified in the contract whether data processor uses any third parties (sub-processors) to help it process the personal data, and if so, which third parties.* *Data controller hereby authorises data processor to hire other sub-*

							processors to meet its obligations under the processing agreement. *Data processor shall notify data controller of any changes concerning the addition or replacement of the third parties (sub-processors) hired by data processor, e.g. through an amendment. Data controller shall be entitled to object to such changes . Data processor shall ensure that any third parties it hires shall commit to ensuring the same level of personal data protection as the security level data processor is bound to provide to the data controller pursuant to the contract.'*
17	**Annex**	**2**	**2, 3**	**4**	**(b)**	Where the data importer engages a sub-processor for carrying out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract which provides for the same data protection obligations as the ones binding the data importer under these Clauses […]	After the words "the same" the words "or similar" should be inserted. In practice this clause that stems from the literal text in the GDPR is very unpractical. In practice it is impossible to agree to exactly the same obligations with a subcontractor. They can be comparable and have the same (or even a better) effect for the controller, but not exactly the same. E.g. if a SaaS-service provider uses a hosting party to deliver the service, then the safety measures by the hosting party in practice are very high level, but not exactly the same as the ones the service provider has agreed to.
18	**Annex**	**2**	**2, 3**	**4**	**(c)**	The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and	This clause does not take into account the different cloud structures with multiple parties, which, in software-solutions, are the current standard in the digital world of today. In these cloud

						subsequent amendments to the data exporter.	structures it is not workable to obtain copies of the processing agreement of all the parties involved.
19	**Annex**	**2**	**2, 3**	**4**	**(d)**	The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.	This clause also fails to take into account the multiple-party cloud-structures. Being 'fully responsible' for this cloud is not feasible. Also, 'any failure' is too wide a scope. The controller only needs to be notified of failures that lead to a personal data breach.
20	**Annex**	**2**	**2, 3**	**9**	**(a)**	(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer, namely [Specify Supervisory Authority and Member State], shall act as competent supervisory authority. [Where the data exporter is not established in a Member State, but falls within the territorial scope of application of the GDPR according to its Article 3(2): The supervisory authority of the Member State where the data subjects whose personal data are transferred under these Clauses in relation to the offering of goods or	Ahead of processing, it is not always clear who the competent DPA will be. Clarifying this in the processing agreement beforehand is not feasible.

						services to them, or whose behaviour is monitored, are located, namely [Specify Member State], shall act as competent supervisory authority.] (b) The data importer agrees to submit itself to the jurisdiction of the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to inquiries, submit itself to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.	
21	**Annex**	**3**		**1**	**As a whole, plus (b), (c)**	(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is notwithstanding Clause 2(f) of Section II. (c) The data exporter shall be entitled to terminate the contract where: (i) the	This clause should also provide the processor the possibility to terminate the clauses. Also, this clause should make a reference to the main agreement between the controller and processor, which often contains the arrangements regarding termination. The clause should only state 'reasonable time'. A month can be way too long, depending on the service provided (and can be

						data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month, (ii) the data importer is in substantial or persistent breach of these Clauses, or (iii) the data importer fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under these Clauses, In this case, it shall inform the competent supervisory authority of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the responsible Party, unless the Parties have agreed otherwise.	specified in e.g. a service level agreement). What exactly is a substantial or persistent breach?
22	**Annex**	**3**		**2**		[OPTION 1: These Clauses shall be governed by the law of one of the Member States of the European Union, provided such law allows for third party beneficiary rights. The Parties agree that this shall be the law of _____ (specify	We understand that Parties can contractually arrange this, but this could lead to impractical situations in practice.

						Member State).] [OPTION 2 (for Module Two and Three): These Clauses shall be governed by the law of the Member State of the European Union where the data exporter is established. Where such law does not allow for third party beneficiary rights, they shall be governed by the law of another Member State of the European Union that allows for third party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).]	
23	**Annex I.A: LIST OF PARTIES**					[…] Signature and date: … […]	Demanding a signature leads to an unnecessary administrative burden and is not required in general contract law.
24	**Annex II: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY**						[DESCRIBE **REQUIREMENTS FOR DATA QUALITY** […] **DATA RETENTION** […] **ACCOUNTABILITY** […] **DATA PORTABILITY AND DATA DISPOSAL**]: according to the GDPR, it is an obligation for the controller to specify these requirements. The processor should clearly inform the controller about their service and their standard operating procedures, but the processor should not decide the requirements.

	OF THE DATA						