Feedback from NLdigital on the Annex to the Commission implementing decision on standard contractual clauses between controllers and processors under Article 28 (7) GDPR and Article 29(7) of Regulation (EU) 2018/1725 (ref. Ares(2020)6654429 - 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 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. We have some remarks that we would like to point out. The general remarks are elaborated on here below. The in-depth comments can be found in **Annex I**. We are happy to be able to provide suggestions.

1. 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 the processing agreement 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 both the controller and the processor. In addition to this, there are several options or blank spaces integrated halfway in the standard clauses where parties must provide input (e.g. choose option one

or option two). These input fields should be transferred over to the subject matter. This prevents parties from overlooking these components. It should be evident that there is nothing to modify in the standard clauses, and that all substantive input belongs at the beginning of the contract.

Furthermore, clause 1 (d) states that annexes I to VII form an integral part of the clauses, and clause 2 (a) states that the clauses cannot be modified. It is not clear what this means for the required ongoing plan-do-check-act cycle (as reflected in f.i. article 24 (1) and 32 (1) the GDPR). Even though clause 2 (b) states that parties can add other clauses or additional safeguards (provided that they do not contradict), this provides insufficient flexibility for adopting a risk-based approach and updating existing measures in order to adapt to changing circumstances. It is therefore recommendable to separate the annexes from the clauses, in order to enable a more flexible approach to the processing agreement.

2. One-sided perspective, disadvantage for SMEs

The clauses are drafted from a one-sided perspective: the perspective of the controller. The responsibilities and obligations of the controller are virtually not specified and the interests of the processor are insufficiently acknowledged. With the current perspective of the SCCs, SMEs in the EU are unnecessarily disadvantaged. There is a significant risk that processors will not agree to applying these SCCs, which could make them void. Small companies that are unable to draft their own agreements could be at a disadvantage, while in fact these are the companies that should be supported and should benefit from these SCCs. There needs to be an appropriate balance and a clear demarcation between the responsibilities of the processor and controller. With this in mind, we developed our Data Pro Code and the accompanying processing agreement. Our processing agreement fulfils both the interests of the controller and the needs of the processor, with special regard to SMEs acting as processor. We strove to relieve them from an unnecessary administrative burden, in line with article 40 GDPR, ‘taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises’. This balance of interests is currently insufficiently reflected in the draft SCCs.

3. Uneven allocation of obligations

As stated before, the responsibilities and obligations of the controller are virtually not specified. Additionally, obligations of the controller are being (wrongfully) imposed on the processor. For example, according to article 28 GDPR, the controller has an obligation to: ‘use only processors providing sufficient guarantees to implement appropriate technical and organisational measures’. This means that the controller needs to decide, and is responsible for this decision, whether a processor provides an appropriate service for the use and purpose the controller has envisioned.

It should be the other way around: the processor needs to inform the controller very clearly about the specifics of its service, for what use it is suited, and what its adopted (security) measures are. If necessary, it is up to the controller to ask for further information. The controller can then make an informed decision if he can employ the processor for his intended purpose of processing. This way, the controller takes his responsibility and complies with his obligations as laid down in the GDPR.

This division of roles and obligations between the controller and the processor should, at all times, be apparent. Processors should support the controller in complying with his obligations, but these obligations cannot be passed on to the processor. It is not clear how the controller can demonstrate compliance (as stated in clause 7.4 (a) in

the draft SCCs) if his obligations are reallocated or not specified. When a fair division is being set out clearly, only then it is possible for both the controller and processor to demonstrate their compliance with the clauses and their compliance with the GDPR.

In order to ensure that the SCCs will be useful 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 detract from other Charter rights of EU organisations. Maintaining a risk based approach is a natural extension of the GDPR, of which a risk based approach is a recurring theme.

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*	*Sub*	*Original text*	*Remark*
1	**Clause 1**	**(d)**	Annexes I to VII form an integral part of the Clauses.	Begin the document with the subject matter and make this more flexible. See general remark 1 + 2.
2	**Clause 2**	**(a)**	The Parties undertake not to modify the Clauses.	Begin the document with the subject matter and make this more flexible See general remark 1 + 2.
3	**Clause 6**		The details of the processing operations, and in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the data controller, are specified in Annex II.	Clause 6 states that the 'purposes of processing' should be specified in annex II. However, it is not necessary for a processor to know the specific purposes for which his clients use his (standard) SaaS service. And it does not work in practice and creates an unnecessary

				administrative burden. If we look the example of a processor who provides a standard SaaS service to its customers, he can provide information in a (standard) annex regarding the 'nature of the processing'(see art. 28 sub 3e), because that relates to the way he set up the service. If parties have to document every specific purpose by each and every client, then this is an extra administrative burden, which does not serve a purpose.
4	**Clause 7**	**(b)**	The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.	Processors have a general duty of care: this is already covered by general contract law. Explicitly stating this is an obligation too far-reaching for the processor: in combination with the wording of clause 10 (b) (1), not complying with clause 7 (b) becomes a ground for terminating the

				clauses, which is too strict.
5	**Clause 7**	**(a)**	The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions are specified in Annex IV. Subsequent instructions may also be given by the data controller throughout the duration of the processing of personal data. Such instructions shall always be documented.	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 II 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.
6	**Clause 7.1**		The data processor shall process the personal data only for the specific purpose(s) of the	With this wording, the obligation of purpose limitation

			processing, as set out in Annex II [Details of the processing operation].	is wrongfully imposed on the processor. 'Specific purposes' is too far-reaching. **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 IV [INSTRUCTIONS FROM THE DATA CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA].'*
7	**Clause 7.2**		Processing by the data processor shall only take place for the duration specified in Annex II. Upon termination of the provision of personal data processing services or termination pursuant to Section III Clause 10, the data processor shall	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.

			[OPTION 1] delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so / [OPTION 2] return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.	**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.'* This clause 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 Clause 7.2, it shall be entitled to invoice data controller for said costs. Further arrangements relating to this subject can be laid down in the contract.'*
8	**Clause 7.3**	**(a)**	The data processor shall implement the technical and organisational measures specified in Annex III to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (personal data breach). In assessing the appropriate level of security, they shall in particular 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. In the event of a personal data breach concerning data processed by the data processor, it shall notify the data controller without undue delay and at the latest within 48h after having become aware of the breach. Such notification shall contain the details of a contact point where more information concerning the personal data breach can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and data records concerned), its likely	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

			consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. Where, and insofar 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 as it becomes available without undue delay.	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.' To notify the controller at the latest within 48h is more restrictive than the GDPR requires in article 33 (2). Also, 48h can be either way too long or way too tight, depending on the service provided. Fixing the term at 48 hours will lead to more administrative burden on both sides, because it will lead to incomplete information from processor to controller and therefor incomplete notifications to the authorities, which will then lead to loads of corrections on notifications. There is a reason why the text in the

				GDPR says without undue delay and for controllers where feasible, not later than 72 hours after having become aware of it'.
9	**Clause 7.3**	**(b)**	The data processor shall cooperate in good faith with and assist the data controller in any way necessary to enable the data controller to notify, where relevant, the competent data protection authority and the affected data subjects, taking into account the nature of processing and the information available to the data processor.	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 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	**Clause 7.3**	**(c)**	The data processor shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. The data processor shall ensure that persons authorised to process the personal data received 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.'
11	**Clause 7.4**	**(a)**	The Parties shall be able to demonstrate compliance with these Clauses.	The obligations of the controller are virtually not specified. It is not clear how the controller can demonstrate compliance this way.
12	**Clause 7.4**	**(b)**	(b) The data processor shall deal promptly and properly with all reasonable inquiries from the data controller that relate to the processing under these Clauses. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and that are stemming directly from Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 and at the data controller's request, allow for and contribute to reviews of data files and documentation or of audits of the processing activities covered by these Clauses, in particular if there are indications of non-compliance.	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.'
13	**Clause 7.4**	**(c)**	The data controller may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the data processor. Where the data processor mandates an audit, it has to bear the costs of the independent auditor. Audits may also include inspections at the premises of the data processor and shall be carried out with reasonable notice.	Other forms of demonstrating compliance by the data processor should be added. **Addition proposed:** *'Data Processor shall be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid equivalent certificate or audit report (third-party memorandum) issued by an independent expert.'*
14	**Clause 7.4**	**(d)**	The data processor and data controller shall make the information referred to in this Clause, 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.'
15	**Clause 7.5**		If the processing involves 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 and offences (special categories of data), the data processor s hall apply specific restrictions and/or the additional safeguards laid down in Annex V.	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.'
16	**Clause 7.6**	**(a)**	OPTION 1 SPECIFIC PRIOR AUTHORISATION: The data processor shall not subcontract any of its processing operations performed on behalf of the data controller under these Clauses to a sub-processor, without its prior specific written agreement. The data processor 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 controller can be found in Annex VI. The Parties shall keep Annex VI up to date. OPTION 2: GENERAL WRITTEN AUTHORISATION The data processor has the data controller's general authorisation for the engagement of sub-processors. The list of sub-processors the data processor intend to engage is be found in Annex VI. The data processor shall inform in writing the data controller 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 controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The Parties shall keep Annex VI up to date.	Option 1 is too restrictive. 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	**Clause 7.6**	**(b)**	Where the data processor engages a sub-processor for carrying out specific processing activities (on behalf of the data controller), it shall do so by way of a contract which imposes on the sub-processor the same obligations as the ones imposed on the data processor under these Clauses. The data processor shall ensure that the sub-processor complies with the obligations to which the data processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 / Regulation (EU) 2018/1725.	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	**Clause 7.6**	**(c)**	The data processor shall provide, at the data controller's request, a copy of such a sub-processor agreement and subsequent amendments to the data controller.	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 structures it is not workable to obtain copies of the processing agreement of all the parties involved.
19	**Clause 7.6**	**(d)**	The data processor shall remain fully responsible to the data controller for the performance of the sub-processor's obligations under its contract with the data processor. The data processor shall notify the data controller 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	**Clause 7.7**	**(a)**	Any transfer of data to a third country or an international organisation by the data processor shall be undertaken only on the basi s of documented instructions from the data controller.	This clause should also refer to Annex VI: list of sub-processors.
21	**Clause 8**	**(c)**	In addition to the data processor's obligation to assist the data controller pursuant to Clause 8(b), the data processor shall furthermore assist the data controller in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to the data processor: (1) The obligation to notify a personal data breach to the competent supervisory authority [INDICATE THE NAME OF THE COMPETENT DPA] without undue delay after having become aware of it, (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons); (2) the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons; (3) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons; (4) the obligation to consult the competent supervisory authority [INDICATE THE NAME OF THE COMPETENT DPA] prior to	A personal data breach is not a data subject right, including this in clause 8 is confusing. Furthermore, personal data breach is already covered in clause 7.3 (a), and in clause 9. It is preferable to incorporate texts about personal data breach in one clause. 'Assist' is too wide a scope. 'Reasonable assist' is preferable. 'Information available' is too wide a scope. 'Necessary

			processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.	information' is preferable. Ahead of processing, it is not always clear who the competent DPA will be. Clarifying this in the processing agreement beforehand is not feasible. Sub (4), prior consultation, is also not a data subject right, including this in clause 8 is confusing. Sub (4) imposes an obligation too wide a scope on the processor. Preferable the text should state that the processor needs only to inform the data controller if the processor has reason to believe that the controller should consult the DPA.

				This clause should take into account the potential costs for the processor (e.g. the possibility for the processor to charge the hourly rate).
22	**Clause 8**	**(d)**	The Parties shall set out in Annex VII the appropriate technical and organisational measures by which the data processor is required to assist the data controller in the application of this Clause as well as the scope and the extent of the assistance required.	Here, a reference to codes of conduct and certifications that guarantee an appropriate level of 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.'
23	**Clause 9**		In the event of a personal data breach, the data processor shall cooperate in good faith with and assist the data controller in any way necessary for the data controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, taking into account the nature of processing and the information available to the processor.	The obligation of the controller to notify data subjects is missing.
24	**Clause 10**	**(b)**	The data controller shall be entitled to terminate these Clauses where: (1) the processing of personal data by the data processor has been temporarily suspended by the data controller pursuant to point (a) and compliance with these Clauses is not restored within a reasonable time and in any event within one month; (2) the data processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 / Regulation (EU) 2018/1725; (3) the data processor fails to comply with a binding decision of a competent court or the competent supervisory authority [INDICATE THE COMPETENT DPA] regarding its obligations under these Clauses or under Regulation (EU) 2016/679 / Regulation (EU) 2018/1725.	This clause should also provide the processor the possibility to terminate the clauses. Also, this clause should make a reference to the main / master 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 specified in e.g. a service level agreement). What exactly is a substantial or persistent breach?
25	**Annex I**		[…] Signature and accession date […]	Demanding a signature leads to an unnecessary administrative burden and is not required in general contract law.
26	**Annex II**		Purpose(s) for which the personal data is processed on behalf of the controller Duration of the processing Categories of data subjects whose personal data is processed …….. Categories of personal data processed …….. Special categories of personal data processed (if applicable) Record(s) of processing	In Annex II, the processor needs to inform the controller very clearly 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 service provided by the

			Place of storage and processing of data	processor will be appropriate and if he can employ the processor for his intended purpose of processing. Regarding **purpose**: it is not necessary for a processor to know the specific purposes for which his clients use his (standard) SaaS service. And it does not work in practice and creates an unnecessary administrative burden. If we look at the example of a processor who provides a standard SaaS service to its customers, he can provide information in a (standard) annex regarding the 'nature of the processing'(see art. 28 sub 3e), because that relates to the way he set up the service. If parties have to document every specific purpose by each and every client, then this is an extra administrative

				burden, which does not serve a purpose. Regarding **duration, data subjects, (special) categories of data**: it is up to the controller to determine this, and on that basis decide if the service the processor delivers is suitable (see above). Regarding **place of storage and processing**: this does not take into account the digital world of today. Data is not stored at just one place. You can specify the data centres, but then it is still not stored at just one place. The only thing that needs to be specified if the data is transferred to third countries. This should be added in Annex VI (list of sub-processors).

27	**Annex III**		Description of the technical and organisational security measures implemented by the data processor(s) […].	[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.
28	**Annex IV**		INSTRUCTIONS FROM THE DATA CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA	Annex IV should not state the substantive instructions, but the arrangements regarding procedures (how should the instructions be given). Misinterpretation of the instructions needs to be

				prevented. Therefore, more guidance is needed.
29	**Annex VI**		LIST OF SUB-PROCESSORS	Here, the text should include whether the sub-processors are established outside the EU.
30	**Annex VII**		APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES BY WHICH THE DATA PROCESSOR IS REQUIRED TO ASSIST THE DATA CONTROLLER	This wording is too generic and therefore Annex VII risks becoming meaningless. Annex VII should state in what way the controller expects the processor to assist the controller in case of a personal data breach or a DPIA.
ADDITIONAL REMARKS				
		text	explanatory	
31	**Proposed addition**	*"Administrative fines imposed on the data controller by the Data Protection Authority cannot be recovered from Data processor."*	We experience that often, controllers want to pass administrative fines from the DPA on to their processor(s). This is unfair, given that when *a controller* receives a fine, the cause of these fines (a breach of the GDPR) is not attributable to the processor. Because if the cause of the fine would be attributable to the processor, the DPA would have imposed that fine on the processor itself. Also, these fines are tailored to annual turnover: if the controller is a multinational and the processor a small, local company, this has severe consequences for the processor. Furthermore, in practice, the processor could be subject to two fines this way (if both the controller and the processor breached the GDPR), which is an undesirable situation.	