EUROPEAN
COMMISSION

Brussels, XXX
[…](2020) XXX draft

ANNEX

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

Commented [A1]: The title is not perfectly aligned with the one of the implementing Decision. See the comment made comment under the Draft implementing act.

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

(b) The data controllers and data processors listed in Annex I ['The Parties'] have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and Article 29 (3) and (4) Regulation (EU) 2018/1725, which require the processing by a processor(s) to be governed by a contract or other legal act under Union or Member State law.

Commented [A2]: To ensure consistency with the wording of art. 28(3) of the GDPR.

(c) These Clauses apply with respect to the processing of personal data as specified in Annex II [Description of the Processing(s)].

(d) Annexes I to VII form an integral part of the Clauses.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses.

(b) This does not prevent the Parties to include the standard contractual clauses laid down in this Clauses in a wider contract, and to add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 respectively or prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a conflict between these Clauses and the provisions of any other agreement between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

[DOCKING CLAUSE] – Optional

(a) Any entity which is not a Party to the Clauses may, with the agreement of all the Parties, accede to these Clauses at any time either as a data controller or as a data processor by completing Annex I [list of Parties], Annex II [description of the processing(s)] and Annex III [technical and organisational measures].

(b) Once Annex I is completed and signed and Annexes II and III are completed, the acceding entity shall be treated as a Party to these Clauses and shall have the rights and obligations of a data controller or a data processor, in accordance with its designation in Annex I.

Commented [A3]: In order to ensure that the Annexes are completed before the new entity accedes to the Clauses.

(c) The acceding entity shall have no rights or obligations arising from the period prior to the date of signing Annex I.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

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.

Clause7

Obligations of the Parties

(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; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. 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.

(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.

7.1. Purpose limitation

The data processor shall process the personal data on behalf of the data controller and only for the specific, explicit and legitimate purpose(s) of the processing specified by the data controller, as set out in Annex II [Details of the processing operation].

7.2. Erasure or return of data

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 at the choice of the controller

[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.

7.3. Security of processing

Commented [A4]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A5]: For the sake of clarity, the EDPB and the EDPS recommend aligning the wording on Article 5 (1) (b) GDPR.

Commented [A6]: For the avoidance of doubt, the EDPB and the EDPS recommend specifying that the purposes of the processing are set by the data controller.

Commented [A7]: The EDPB/EDPS suggest further clarifying that the purposes of processing are set by the controller in accordance with Article 28 (3) GDPR.

Commented [A8]: We suggest that a reference to the storage limitation principle should be added in this clause.

Commented [A9]: We suggest the inclusion of this wording ("at the choice of the controller") in order to more closely match the wording of Article 28 (3) (g) GDPR.

Commented [A10]: The EDPB and the EDPS suggest replacing "certify" with "demonstrate" to avoid any confusion with certification.

Commented [A11]: Please see the comment made on this point in the Joint Opinion.

(a) The processor shall, together with the controller, to which they shall provide assistance as necessary, assess and implement the appropriate level of security, taking into account the risks entailed by the processing for the rights and freedoms of the persons whose personal data are processed, the nature of the personal data, the nature, scope, context and purposes of the processing as well as the state of the art and the cost of implementation of the identified security measures. The processor shall at least 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~~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 [NUMBER OF HOURS] after the data processor becoming aware of the data breach~~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 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 further delay.

(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~~ the personal data breach and the information available to the data processor.

(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~~Clauses. 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.

7.4. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(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, systems, and documentation, and allow for and contribute to ~~or of~~ audits of the

Commented [A12]: We believe that the definition of data breach has in any case to be brought in line with the text of art. 4 (12) of the GDPR and the EUDPR: "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Commented [A13]: We would suggest to reorganise and reword this paragraph.

The first obligation is to identify measures upon a risk-based approach and assist the controller. Then the clauses might want to specify those measures the controller has already identified. Yet, the obligation for the identification of measures based on the risks remain also incumbent also on the processor independently from the conclusions reached by the controller.

A possible text, completely replacing what is proposed ("The data processor ... purpose of processing") is proposed directly in the text.

Commented [A14]: Please see the remarks made in the Joint Opinion concerning this clause

Commented [A15]: Wording aligned with Art. 33 (4) GDPR.

Commented [A16]: The EDPB and EDPS suggest that as there is a specific Clause on data breach notification these developments might not be needed in this Clause but would be better placed in Clause 9.

Commented [A17]: The EDPB and EDPS do not see the need for such specification which is not present in the GDPR

Commented [A18]: To align with the wording of Art. 33 (3) (a) and 34 (2) GDPR.

Commented [A19]: Editorial suggestion for consistency with the rest of the text.

Commented [A20]: The term "*reasonable*" is likely to raise a lot of questions and is subject to interpretation. In addition, stating that the processor shall deal with reasonable inquiries only also seems in contradiction with the obligation stated in the subsequent paragraph that the processor shall make available to the controller all information necessary to demonstrate compliance in accordance with Art. 28 (3) (h) GDPR.

Commented [A21]: Such addition seems necessary to better reflect what may be subject to an audit.

Commented [A22]: The wording suggests that only a review of audit would be allowed. The proposal aims to reflect the provisions of Art. 28 (3) (h) GDPR that are relevant in this context.

processing activities covered by these Clauses~~, in particular if there are indications of non-compliance~~.

(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 or the physical facilities of the data processor ~~and shall be carried out with reasonable notice~~.

(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.

7.5. Special categories of personal data

If the processing involves i) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, ii) genetic data, iii)~~or~~ biometric data for the purpose of uniquely identifying a natural person, iv) data concerning health or v) data concerning a person's sex life or sexual orientation, or vi) data relating to criminal convictions and offences (special categories of data), the data processor shall apply specific restrictions and/or the additional safeguards laid down in Annex V.

7.6. Use of sub-processors

(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. In order to make the assessment and the decision whether to authorise sub-contracting, the data processor shall provide the data controller with all necessary information on the intended sub-processor, including on their locations, the processing activities they will be carrying out and on any safeguards and measures to be implemented. 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 specifically 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). In order to make the assessment and the decision whether to authorise sub-contracting, the data processor shall provide the data controller with all necessary information on the intended sub-processor, including on their locations, the processing activities they will be carrying out and on any safeguards and measures to be implemented. The Parties shall keep Annex VI up to date.

(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, and these should be binding as a matter of EU or

Commented [A23]: This part seems unnecessary, as the processor must in any case participate in audits or inspections, regardless of the (non)existence of indications of non-compliance. Also, this might be misunderstood to restrict the statutory audit right.

Commented [A24]: The right of audit of the controller should not be limited to premises of the processor but should also cover the places where the processing is carried out. This may be the case of the processor's physical facilities.

Commented [A25]: The EDPB and EDPS wonder whether imposing a requirement for the controller to give the processor reasonable notice applies in each and every case.

Commented [A26]: We suggest referring to "genetic data" separately like Article 9 GDPR does.

Commented [A27]: We think this mirrors the wording of the GDPR more accurately.

Commented [A28]: It should be specified that these specific restrictions or specific safeguards should be in accordance with the specific instructions or guarantees requested by the controller. The processor should not decide on its own what such safeguards can be in line with Article 28 (3) GDPR which imposes compliance with controller instructions.

Commented [A29]: We would recommend to include this new sentence to reflect the following recommendation from the EDPB C-P GLs, p. 39, par 148: "*In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor*[54]. [54] *This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.*"

Commented [A30]: Therefore, the EDPB and the EDPS call on the Commission to provide for an obligation to inform data subjects of their right to request the restriction of the processing of their data.

Commented [A31]: We suggest that it should be specified that the time period must be long enough to ensure the controller has a meaningful right to object.

Commented [A32]: We would recommend to include this new sentence to reflect the following recommendation from the EDPB Guidelines on the concepts of controller and processor in the GDPR, p. 39, par 148: "*In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor. This* ... [1]

Commented [A33]: We are of the opinion that the legal consequences of an objection to a new sub-processor should be further detailed in the contract. In particular, it has to be clear that in the case of an objection the processor shall not engage the sub-processor. ... [2]

Commented [A34]: In line with Art. 28 (4) GDPR and Art. 29 (4) EUDPR, obligations shall be imposed on the other processor by way of contract or other legal act under Union or Member State law.

Member State law. 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.

(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.

(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.

(e) The data processor shall agree a third party beneficiary clause with the sub-processor whereby - for instance in the event of bankruptcy of the data processor - the data controller shall be a third party beneficiary to the sub-processor contract and shall have the right to enforce the contract against the sub-processor, including where applicable by instructing the sub-processor to erase or return the personal data.

~~(d)~~(f) Prior to processing, the data processor shall inform the sub-processor of the identity and contact details of all controllers for which the sub-processor processes personal data.

7.7. International transfers

(a) Any transfer of data to a third country or an international organisation by the data processor shall be undertaken only on the basis of documented instructions from the data controller listed in Annex IV or a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The data controller agrees that where the data processor engages a sub-processor in accordance with Clause 7.6. for carrying out specific processing activities (on behalf of the data controller) in a third country or international organisation and those processing activities involve transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor may use standard contractual clauses adopted by the Commission on the basis of Article 46(2) of Regulation (EU) 2016/679 in order to comply with the requirements of Chapter V of Regulation (EU) 2016/679, provided the conditions for the use of those clauses are met and the sub-processor is able to comply with all stipulations of those clauses.

Clause 8

Data subject rights

(a) The data processor shall promptly notify the data controller about any request received directly from the data subject. It shall not respond to that request itself, unless and until it has been authorised to do so by the data controller.

(b) Taking into account the nature of the processing, the data processor shall assist by appropriate technical and organisational measures, insofar as this is possible, the data controller in fulfilling its obligations laid down in Chapter III of the GDPR, in particular to respond to data subjects' requests for the exercise of their rights, namely:

(1) the right to be informed when personal data are collected from the data subject,

Commented [A35]: The EDPB and the EDPS suggest the inclusion of this clause. A similar clause was also present in the Danish and Slovenian SCCs.

Commented [A36]: The EDPB and EDPS are of the opinion that this information would need to be provided. This should also be specified in the Annexes as parties should be requested to provide the information in the annexes..

Commented [A37]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A38]: We suggest the inclusion of references to Regulation 2018/1725. When EUIs engage processors and allow transfers from processor of EUIs to recipients a third country or international organisation, references only to GDPR are not correct, rather references to the EUDPR should also be made.

Commented [A39]: We suggest the inclusion of this wording to ensure alignment with the wording of Article 28 (3) (a) GDPR.

Commented [A40]: The use the SCCs – even if the conditions for their use are met – is not sufficient if the subprocessor is not able to comply with them. Otherwise, an onward transfer to a third country which normally would require supplementary measures might be permitted without supplementary measures.

Commented [A41]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A42]: The proposed changes aim at bringing the text in line with the text of the GDPR and also clarifying that the assistance is not always linked to a request from the data subject (for instance for items 1, 2 and 10 of the list).

(2) the right to be informed when personal data have not been obtained from the data subject,

(3) the right of access by the data subject,

(4) the right to rectification,

(5) the right to erasure ('the right to be forgotten'),

(6) the right to restriction of processing,

(7) the notification obligation regarding rectification or erasure of personal data or restriction of processing,

(8) the right to data portability,

(9) the right to object,

(10) the right not to be subject to a decision based solely on automated processing, including profiling.

(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) ~~t~~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 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.

(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.

Clause 9

Notification of personal data breach

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.

Commented [A43]: The EDPB and the EDPS invite the European Commission to include a point referring to the obligations of security under Article 32 GDPR and the obligations of security and confidentiality under Articles 33, 36, 37, 38, 41 EU DPR (to reflect the wording of Article 28 GDPR and Article 29 EU DPR).
Please also see paragraph 49 of the Joint Opinion.

Commented [A44]: Please see the remarks made in the Joint Opinion concerning this clause.

Commented [A45]: The EDPB and the EDPS are not sure to fully understand the distinction between Annexes III and VII.

To distinguish from Annex III, Annex VII could provide details on how the processor is to provide assistance to the controller to comply:
- with controller's obligations to respond to requests for exercising data subject's rights laid down in Chapter III of the GDPR and Chapter III of the EUDPR and
- with controller's obligations under Arts. 32 to 36 GDPR and Arts. 33 to 41 EUDPR

Commented [A46]: The requirements to notify a competent authority (and name the competent authority), which are now addressed under clause 7.3, letter (a), clause 8 (c) (1) and clause 9 could be addressed under one clause (i.e. clause 9) in order to avoid repetition.

Commented [A47]: The EDPB and EDPS do not see the need for such specification which is not present in the GDPR

(a) In accordance with Clause 8(c~~b~~) the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, where relevant [INDICATE THE NAME OF THE COMPETENT DPA]. The data processor shall be required to assist in obtaining in particular the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679 or under Articles 34(3) Regulation (EU) 2018/1725, shall be stated in the data controller's notification:

(1) The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(b) The Parties shall set out in Annex VII all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

SECTION III – FINAL PROVISIONS

Clause 10

Termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 / Regulation (EU) 2018/1725, in the event that the data processor is in breach of its obligations under these Clauses, the data controller may instruct the data processor to temporarily suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The data processor shall promptly inform the data controller in case it is unable to comply with these Clauses, for whatever reason.

(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.

Commented [A48]: Letter (c) is the correct reference.

Commented [A49]: Corresponding to wording of Art. 33 (3) GDPR.

Commented [A50]: The EDPB and the EDPS are of the view that the European Commission should make clear that in case of termination of the Clauses the provisions of Clause 7.2 (Erasure or return of personal data) apply.

Commented [A51]: In the view of the EDPB/EDPS, it is not needed in this context to explicitly request the parties to name the competent SA.

ANNEX I LIST OF PARTIES

Commented [A52]: Please see the remarks made in the Joint Opinion concerning this Annex.

Data controller(s): [*Identity and contact details of the data controller(s), and, where applicable, of the data controller's representative in the Union designated pursuant to Article 27 Regulation (EU) 2016/679]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

2.

…

Data processor(s): [*Identity and contact details of the data processor(s)]*

1. Name: …

Address: …

Contact person's name, position and contact details: …

Signature and accession date: …

2.

…

ANNEX II: DESCRIPTION OF THE PROCESSING

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

Place of storage and processing of data

……

……

……

Subject-matter of the processing

……

Commented [A53]: The EDPB and EDPS suggest that the European Commission add some explanatory text on Annex 2, similar to the one that was included in the SCCs prepared by the Danish SA and the Slovenian SA. This text should, more specifically, require the parties to include a sufficiently detailed description of the categories of personal data. For instance, the explanatory text included in the aforementioned SCCs included a request to describe the type of personal data being processed, with some examples, and the note that the description should be made in the most detailed possible manner and in any circumstance the types of personal data must be specified further than merely "personal data" or "Article 9 / 10 data".

Commented [A54]: The EDPB and the EDPS do not understand what this means and therefore suggest either deletion or clarification.

Commented [A55]: The EDPB and the EDPS suggest adding a clarification as to what "place" means – e.g. just the country or the exact names and addresses of the facilities where the personal data will be processed.

Commented [A56]: We suggest to request the parties to detail the subject matter of the processing in the Annex in order to be in line with the wording of Article 28 (3) GDPR.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational ~~security~~ measures implemented by the data processor(s)

Commented [A57]: In our view, this should be deleted, since now this list includes all measures, not only the security-related ones.

[TAKING INTO ACCOUNT THE NATURE, SCOPE, CONTEXT AND PURPOSES OF THE PROCESSING ACTIVITY AS WELL AS THE RISK FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS, DESCRIBE ELEMENTS THAT ARE ESSENTIAL TO ~~THE~~ ENSURE AN ADEQUATE LEVEL OF SECURITY]

Commented [A58]: Clarification.

Where necessary:
[DESCRIBE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES]

[DESCRIBE REQUIREMENTS FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT]

[DESCRIBE REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING]

[DESCRIBE REQUIREMENTS FOR USERS I~~N~~DENTIFICATION AND AUTHORISATION]
[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE]

[DESCRIBE REQUIREMENTS FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED]

[DESCRIBE REQUIREMENTS FOR EVENTS LOGGING]

[DESCRIBE REQUIREMENTS FOR SYSTEM CONFIGURATION, INCLUDING DEFAULT CONFIGURATION]

[DESCRIBE REQUIREMENTS FOR INTERNAL IT AND IT SECURITY GOVERNANCE AND MANAGEMENTS]

[DESCRIBE REQUIREMENTS FOR CERTIFICATION / ASSURANCE OF PROCESSES AND PRODUCTS]

[DESCRIBE REQUIREMENTS FOR DATA AVOIDANCE AND MINIMISATION]

Commented [A59]: This term is not used in the GDPR. We wonder whether it has a meaning that goes beyond data minimisation as described in Article 25 (1) GDPR. If so, the term should be explained; if not, it should be deleted.

[DESCRIBE REQUIREMENTS FOR DATA QUALITY]

[DESCRIBE REQUIREMENTS FOR DATA RETENTION]

[DESCRIBE REQUIREMENTS FOR ACCOUNTABILITY]

[DESCRIBE REQUIREMENTS FOR DATA PORTABILITY AND DATA DISPOSAL]

Commented [A60]: This term is not used in the GDPR. We wonder whether it has a meaning that goes beyond data portability as described in Article 20 GDPR. If so, the term should be explained; if not, it should be deleted.

ANNEX IV: INSTRUCTIONS FROM THE DATA CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA

ANNEX V: SPECIFIC RESTRICTIONS AND/OR ADDITIONAL SAFEGUARDS CONCERNING DATA OF SPECIAL CATEGORY

For special categories of personal data processed mentioned in Annex II restrictions or safeguards applied such as:
access restrictions,
keeping a record of access to the data,
restrictions of the purposes for which the information may be processed,
additional security measures (e.g. strong encryption for transmission),
requirement of specialised training for staff allowed to access the information

Commented [A61]: The term "data" seems to be more appropriate unless there is a specific reason why the term "information" has been chosen; in case of a specific reason, it should be explained.

ANNEX VI: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:
Name (full legal name):
Company number:
Address:
Description of the processing (in case several sub-processors are authorised, including a clear delimitation of responsibilities):
Place(s) of processing:
[To be completed for every authorised sub-processor]

The controller will need approve the use of sub-processors. The processor is not entitled – without the express written consent of the controller – to engage a sub-processor for any other processing than the agreed processing or to have another sub-processor perform the described processing.

Commented [A62]: We suggest adding the introduction and the following paragraph in order to remind the parties of the requirements stipulated in the SCCs and the law.

Commented [A63]: Just like with regard to the term in Annex II, we suggest adding a clarification as to what "place" means – e.g. just the country or the exact names and addresses of the facilities where the personal data will be processed.

Commented [A64]: As already mentioned in the Joint Opinion itself, the EDPS and EDPB are of the opinion that it is of utmost importance that the Annexes to the SCCs delimit with absolute clarity the roles and responsibilities of each of the parties in each relationship and with regard to each processing activity. We therefore suggest including further details on the authorised sub-processors and their activities, also reflecting the following recommendation from the EDPB C-P GLs, para. 148:
"In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor. This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR."

ANNEX VII: APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES BY WHICH THE DATA PROCESSOR IS REQUIRED TO ASSIST THE DATA CONTROLLER

Commented [A65]: Similar to Annex III, we suggest adding the requirements to be covered in this Annex. As correctly filling out this Annex might be challenging to the parties, we suggest adding examples of possible measures or detailed descriptions of the expected assistance.

Page 5: [1] Commented [A32] **Author**

We would recommend to include this new sentence to reflect the following recommendation from the EDPB Guidelines on the concepts of controller and processor in the GDPR, p. 39, par 148: "*In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor. This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.*"

Page 5: [2] Commented [A33] **Author**

We are of the opinion that the legal consequences of an objection to a new sub-processor should be further detailed in the contract. In particular, it has to be clear that in the case of an objection the processor shall not engage the sub-processor.