EDPB - EDPS Joint Opinion 1/2021 on the European Commission's Implementing Decision on standard contractual clauses between controllers and processors

for the matters referred to in Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725

TABLE OF CONTENTS

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ("**EUDPR**"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1 BACKGROUND

1. In the context of the relationship between a controller and a processor, or processors, for the processing of personal data, the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "**GDPR**") establishes, in its Article 28, a set of provisions with respect to the setting up of a specific contract between the parties involved, and mandatory provisions that should be incorporated in it.

2. According to Article 28 (3) GDPR, the processing by a processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller, setting out a set of specific aspects to regulate the contractual relationship between the parties. These include the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects, among others. Article 28 (4) provides for additional requirements where a processor engages another processor for carrying out specific processing activities on behalf of the controller.

3. Under Article 28 (6) GDPR, without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred in paragraphs (3) and (4) of Article 28 GDPR may be based, wholly or in part, on standard contractual clauses. These standard contractual clauses are to be adopted for those matters referred to in paragraphs (3) and (4).

4. Article 28 (7) GDPR provides that the Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

5. The EUDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the Union.

6. Article 29 (3), (4) and (7) of the EUDPR contain similar requirements as the ones included in Article 28 (3), (4) and (7) of the GDPR. This is justified by the fact that, in the interest of a coherent approach to

---

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

personal data protection throughout the Union and the free movement of personal data within the Union, the data protection rules applicable to the public sector in the Member States and the data protection rules for Union institutions, bodies, offices and agencies were aligned as far as possible.

2 SCOPE OF THE OPINION

7. On 12 November 2020, the Commission published:

    ʃ a Draft Commission Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725) (the "**Draft Decision**");

    ʃ a draft Annex to the Commission Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725) (the "**Draft SCCs**").

8. The same day, the European Commission also published a draft Commission Implementing Decision and its Annex on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

9. On 12 November 2020, the European Commission requested a joint opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) on the basis of Article 42(1), (2) of Regulation (EU) 2018/1725 (EU DPR) on these two sets of draft standard contractual clauses and the respective implementing acts.

10. For the sake of clarity, the EDPB and EDPS decided to issue two separate opinions on these two sets of SCCs.

11. The scope of this opinion is thus limited to the Draft Decision and Draft SCCs between controllers and processors for the matters referred to in Article 28 (3) and (4) of the GDPR and Article 29 (3) and (4) of the EUDPR.

3 GENERAL REASONING REGARDING THE DRAFT DECISION AND THE DRAFT SCCs

3.1 General comments

12. Any set of SCCs must further specify the provisions foreseen in Article 28 GDPR and Article 29 EUDPR. The opinion of the EDPB and the EDPS aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented Draft SCCs that could serve as standard contractual clauses in compliance with Article 28 (7) GDPR and Article 29 (7) EUDPR.

13. The EDPB and the EDPS are of the opinion that clauses which merely restate the provisions of Article 28(3) and (4) GDPR and Article 29 (3) and (4) EUDPR are inadequate to constitute standard contractual clauses. The Board and EDPS have therefore decided to analyse the document in its entirety, including the appendices. In the opinion of the Board and the EDPS, a contract under Article 28 GDPR or Article 29 EUDPR should further stipulate and clarify how the provisions will be fulfilled. It is in this light that the Draft SCCs submitted to the Board and EDPS for opinion are analysed.

14. Adopted standard contractual clauses constitute a set of guarantees to be used as is, as they are intended to protect data subjects and mitigate specific risks associated with the fundamental principles of data protection.

15. The EDPB and the EDPS welcome in general the adoption of standard contractual clauses as a strong accountability tool that facilitates compliance by controllers and processors to their obligations under the GDPR and the EUDPR.

16. The EDPB already issued opinions on standard contractual clauses prepared by the Danish Supervisory Authority[2] and the Slovenian Supervisory Authority[3].

17. To ensure a coherent approach to personal data protection throughout the Union, the EDPB and the EDPS strongly welcome the envisaged adoption of SCCs having an EU-wide effect by the Commission.

18. The same set of SCCs will indeed apply irrespective of whether this relationship involves private entities, public authorities of the Member States or EU institutions or bodies. These EU-wide SCCs will ensure further harmonisation and legal certainty.

19. The EDPB and the EDPS also welcome the fact that the same set of SCCs should apply in respect of the relationship between controllers and processors subject to GDPR and EUDPR respectively.

3.2　Explanation of the methodology applied and structure of the document

20. For the sake of clarity, the present opinion comprises (i) a core part detailing general comments the EDPB and the EDPS wish to make and (ii) and an annex where comments of a more technical nature are made directly to the Draft Decision and the Draft SCCs in order to provide some examples of possible amendments. There is no hierarchy between the general comments and the technical ones.

21. In addition, the main comments on the Draft Decision and the Draft SCCs are presented in two separate sections. Where needed, cross-references are made to ensure consistency.

22. For the sake of consistency, where needed, cross-references are also made to the EDPB - EDPS Joint Opinion 02/2021 on standard contractual clauses for the transfer of personal data to third countries.

4　ANALYSIS OF THE DRAFT DECISION AND ITS ANNEX

4.1　Main comments on the Draft Decision

4.1.1　On the scope of the Decision and on the articulation with the other set of Draft SCCs on transfers

23. Article 2 of the Draft Decision provides that "*the standard contractual clauses as set out in the Annex may be used in contracts between a controller and a processor who processes personal data on its behalf, where the controller and the processor are subject to Regulation (EU) 2016/679 or Regulation (EU) 2018/1725*".

---

[2] Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf.
[3] Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR): https://edpb.europa.eu/our-work-tools/our-documents/opinjoni-tal-bord-art-64/opinion-172020-draft-standard-contractual_en.

24. The EDPB and the EDPS are of the opinion that the current wording of this Article is source of legal uncertainty, as to the situations in which entities will be able to rely on these SCCs.

25. The EDPB and the EDPS understand that the intention of the Commission is that these SCCs are only meant to cover intra-EU situations and that these clauses should not be relied upon in case of transfer within the meaning of Chapter V. In these cases, parties should rather rely on the separate set of standard contractual clauses that has been established for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 and that is also meant at covering Article 28 (3) and 28 (4) GDPR requirements ("**transfer SCCs**").

26. The EDPB and EDPS consider that the Draft Decision does not provide sufficient clarity to the parties and the exact scope of the Decision has to be clearly set out and detailed in a specific recital of the Draft Decision, for instance before the current Recital 10 of the Draft Decision.

27. Moreover, the Board and the EDPS are of the opinion that the current wording of Article 2 of the Draft Decision does not limit the scope to intra-EU situations as controllers or processors subject to the GDPR for a given processing activity may be established outside the EU by virtue of Article 3 (2) GDPR. It should then be clarified whether these SCCs could be relied upon in this situation.

28. Finally, the EDPB and the EDPS are rather of the opinion that the intended limitation to intra-EU situations is not justified. For example, the EDPB and EDPS do not see any reason to prevent entities from relying on these SCCs – for the sake of complying with Articles 28 (3) and 28 (4) GDPR - if one of the party is not subject to the GDPR for a given processing activity but is located in an adequate country. If the scope of the SCCs is broadened to situations involving transfers outside the EU, it should be made clear to the parties that these SCCs will provide compliance with the requirements under Article 28 (3) and 28 (4) GDPR or 29 (3) and 29 (4) EUDPR but not all the requirements deriving from the GDPR or the EUDPR, for instance on the rules related to international transfers.

29. In the view of the EDPB and the EDPS, it is also important to clearly explain in the Decision the articulation and interplay between this set of SCCs and the transfer SCCs. It should be made clear to the parties, already in the decision, that when parties intend to benefit from SCCs both under Article 28 (7) GDPR and 46 (2) c GDPR, then parties need to rely on transfer SCCs.

4.2 Main comments on the Annex to the Commission implementing decision

4.2.1 Purpose and scope (Clause 1 of the Draft SCCs)

30. **Clause 1 (a)** of the Draft SCCs specifies that the purpose of the SCCs is to ensure compliance with the GDPR and the EUDPR. The EDPB and EDPS are of the opinion that parties to the contract when signing the clauses should be able to choose to select either references to the GDPR or the EUDPR depending on the relevant Regulation applicable to their situation.

31. This way, entities using SCCs under Article 28 GDPR would have no reference to the EUDPR in their SCCs and entities relying on Article 29 EUDPR would avoid the references to the GDPR. This would contribute to bring clarity in the relations between the parties that are often less familiar with such regulations. If so, the SCCs should specify that such choice is possible and adapt the drafting of the SCCs accordingly.

32. As provided for in **Clauses 1 (b) and (c)**, and in accordance with **Clause 5** (Docking clause), several controllers and processors, listed in **Annex I**, can be parties to the SCCs for the processing specified in **Annex II**. The EDPB and EDPS believe that, in such case of multiple parties to the contract, the SCCs (and their Annexes) should require from parties to further detail and delimit the allocation of

responsibilities and indicate clearly which processing is carried out by which processor(s) on behalf of which controller(s) and for which purposes. The current formulation of these clauses of the SCCs and the Annexes may lead to confusion as to the qualification and role of each entity with respect to a given processing operation, especially given the possibility to include a docking clause.

4.2.2   Invariability (Clause 2 of the Draft SCCs)

33.   According to **Clause 2 (b)** of the Draft SCCs, the parties undertake not to modify them unless additional clauses "*do not contradict, directly or indirectly*" the SCCs. To provide controllers and processors with legal certainty, the EDPB and EDPS would welcome clarifications on the type of clauses that the European Commission would consider as contradicting directly or indirectly SCCs. Such clarification could for instance indicate that clauses contradicting SCCs would be those that undermine or negatively impact the obligations in the SCCs or prevent compliance with the obligations contained the SCCs. For example, clauses allowing processors to use the data for its own purposes would be contrary to the obligation of the processor to process personal data only on behalf of the controller, and for the purposes and by the means identified by the latter.

4.2.3   Docking clause (Clause 5 of the Draft SCCs)

34.   **Clause 5** of the Draft SCCs allows, as an option, any entity to accede to the SCCs and therefore to become a new party to the contract as a controller or as a processor. As already mentioned above, the qualification and the role of such new party to the contract should appear clearly in the Annexes by requesting parties to further detail and delimit the allocation of responsibilities and indicate clearly which processing is carried out by which processor(s) on behalf of which controller(s) and for which purposes.

35.   **Clause 5 (a)** makes the accession of new parties to the SCCs conditional upon the agreement of all the other parties. In order to avoid any difficulties in practice, the EDPB and EDPS would welcome a clarification on the way such agreement could be given by the other parties (whether it should be in writing or not, the deadline to provide such agreement, the information needed before agreeing). Also, the EDPB and EDPS would welcome clarification as to whether and how such agreement has to be given by all the parties, irrespective of their qualification and role in the processing.

4.2.4   Obligations of the Parties (Clause 7 of the Draft SCCs)

36.   Although the title of this clause is "Obligations of the Parties", **Clause 7 (a)** in its current form only makes reference to obligations imposed on the processor. Article 28(3) GDPR specifies that the controller/processor contract shall set out the rights, but also the obligations, of the controller. Consequently, the EDPB and EDPS suggest that a reference is added to this clause to the obligations imposed on the controller, for the purposes of completeness and enhanced clarity. For instance, the following sentence could be added before Clause 7 (a): "*The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data and is responsible for ensuring that the processing of personal data takes place in compliance with the applicable EU or Member State data protection provisions and the Clauses (including ensuring that the processing of personal data which the processor is instructed to perform relies on a legal basis pursuant to Article 6 GDPR or Article 5 EUDPR)*".

37.   Clause 7 (a) also provides that instructions should be specified in Annex IV and that subsequent instructions may also be given by the controller. The possibility for the controller to give "*subsequent instructions*" is necessary to fully implement the rights and obligations of the parties set out in the

SCCs, but is not unlimited. Any subsequent instruction should be in line with the respective rights and obligations of the parties set out in the SCCs. The EDPB and the EDPS consider that this should be clearly specified in the Clause.

38. Additionally, in order to enhance consistency with the text of 28 (3) (a) of the GDPR and Article 29 (3) (a) of the EUDPR and to include such obligation directly in the contract, the EDPB and the EDPS suggest amending the end of the first sentence of Clause 7 (a) with the following underlined wording: "*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*".

39. Concerning the event of unlawful instructions given by the controller, described by Article 28 (3) subparagraph 2 GDPR, the EDPB and EDPS are of the opinion that the contract between the controller and the processor should include some more precise information as to the consequences and solutions envisioned in case the processor informs the controller that, in its opinion, the instruction infringes the GDPR or other applicable data protection provisions. Therefore, the European Commission should invite the parties to include further details about the consequences of the notification of an infringing instruction in the contract (e.g. a clause on the possibility for the processor to suspend the implementation of the affected instruction until the controller confirms, amends or withdraws its instruction, a clause on the termination of the contract in case the controller persists with an unlawful instruction).

40. Concerning the options available to the controller pursuant to **Clause 7.2** relating to erasure or return of data, the EDPB and EDPS call on the European Commission to specify in the Clause itself that the controller should be able to modify the choice made at the time of signature of the contract throughout the life cycle of the contract and upon termination.

41. As a general comment on **Clause 7.3** relating to the security of processing**,** the EDPB and EDPS note that all obligations lie on the processor without specifying the role of the controller in particular regarding the assessment of the risk which must be performed for security measures in consideration of the purpose of the processing set by the controller. In some cases, the processor might not be aware of the exact purpose of the processing, for instance when hosting data. Therefore, and in accordance with the provision of Article 28.3 of the GDPR, the EDPB and EDPS are of the opinion that the Clause should be completed with the obligations applying with respect to the security of the processing to the controller which, in particular, has to provide all useful information to the processor to comply with the relevant requirements in this respect**.**

42. **Clause 7.3 (a)** of the Draft SCCs provides that the processor has 48 hours at the latest to notify the controller of a personal data breach. Such delay may be short in some situations and may also trigger confusion with the delay in which the controller has to notify the personal data breach to the SA (which starts when the controller is aware of it, i.e.; when the processor notifies him). While taking into account the requirement for the processor to notify the controller "*without undue delay*" after becoming aware of the personal data breach in accordance with Article 33.2 GDPR, the EDPB and EDPS suggest to leave the parties to provide the appropriate timeframe to meet this requirement, depending on the specific situation. The parties should thus be requested to specify in the SCCs the timeframe agreed for such notification.

43. **Clause 7.4 (c)** of the Draft SCCs provides for the possibility for the controller, in order to conduct audits, to rely on an independent auditor mandated by the processor. This provision is not foreseen

in Article 28 (3) (h) GDPR and needs to be aligned with this article which provides that the processor has to allow for and contribute to audits, including inspections, that are conducted by the controller or another auditor mandated by the controller. As such, the processor might propose an auditor, but the decision about the auditor has to be left to the controller according to Article 28 (3) (h) of the GDPR.

44. **Clause 7.4 (c)** also states that where the controller mandates an independent auditor, it shall bear the costs, and where the processor mandates an audit, it has to bear the costs of the independent auditor. As the issue of allocation of costs between a controller and a processor is not regulated by the GDPR, the EDPB and the EDPS are consequently of the opinion that any reference to the costs should be deleted from this clause.

45. With regard to **Clause 7.7** on international transfers, and more specifically concerning the situation where a processor relies on a sub-processor in a third country, the EDPB and the EDPS express the view that point (b) could be more explicit as to the possibility for these two parties to sign one single set of SCCs which aims at compliance both with Chapter V and Article 28(4) GDPR, if this is indeed the goal this clause would like to achieve, which would require further clarification. Also it should be clarified whether parties then need to rely on this set of SCCs or rather on the transfer SCCs also providing safeguards under Article 28 (3) and (4) of the GDPR.

46. Additionally, the EDPB and the EDPS would like to highlight that while **Clause 7.7 (b)** only refers to the use of the transfer SCCs, several other transfer tools could be legitimately relied upon for framing the transfers from the processor to a sub-processor in a third country, and thus suggest using a more generic formulation referring to transfer tools under Article 46 GDPR.

47. The EDPB and the EDPS also identified the need to further clarify the last part of point (b) of Clause 7.7, referring to "*the conditions for the use of*" the transfer SCCs. As this provision suggests that there may be specific conditions for the use of the transfer SCCs, there is a need to specify what these conditions are.

4.2.5 Data Subject rights (Clause 8 of the Draft SCCs)

48. The clause is currently entitled "*Data Subject rights*" but it is the opinion of the EDPB and the EDPS that the title does not reflect the content of the clause.

49. **Clauses 8 (a) and 8 (b)** of the Draft SCCs indeed refer to the processor's obligation to provide assistance 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. However, Clauses 8 (c) and 8 (d) refer to the assistance of the processor with other types of controller's obligations, in particular under Articles 32 to 36 GDPR and Articles 33 to 41 EUDPR.

50. The EDPB and the EDPS therefore suggest to change the title of this clause to "*Assistance to the controller*" to reflect the different assistance that the processor needs to provide.

51. As an alternative, the EDPB and EDPS would recommend to the Commission to split the clause in two to distinguish between the assistance that the processor needs to provide:

) 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 Articles 32 to 36 GDPR and Articles 33 to 41 EUDPR.

52. Also, Clause 8 (a) of the Draft SCCs provides that "*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*".

53. The EDPS and EDPB are of the opinion that this clause should:

   ⌒ further specify that the responses to data subjects shall be made in accordance with the controller's instructions (e.g. on content of the response) as set out in Annex IV;

   ⌒ further specify that the scope of processor's obligation relating to the exercise of data subject's rights on behalf of the controller should be described and clearly set out in Annex VII.

54. **Clause 8 (c) (1)** as well as **Clause 9 (a)** require to specify the Supervisory Authority which is competent but does not envisage the case where there are several controllers parties to the contract and thus several competent supervisory authorities. Therefore, the possibility to mention several competent supervisory authorities should be added. In addition, there may be cases where the processing subject to the clauses is cross-border and a lead Supervisory Authority is to be identified as competent Supervisory Authority. This should also be reflected in Clauses 8 (c) (1) and 9 (a).

55. The EDPB and EDPS suggest that, in case processors within the EU are bound by third country laws or practices affecting the compliance with these Clauses, the Commission should assess whether an additional clause to address these cases is appropriate.

4.2.6   Annexes to the Draft SCCs

56. The SCCs are designed to be used for data processing agreements, which may involve more than one party as a controller and/or more than one party as a processor. This implies the risk that, if the Annexes are not filled out appropriately, the responsibilities of the parties are blurred. This risk increases where new parties subsequently join the contract by using the Docking Clause and/or the contract covers processing for different purposes or under different circumstances.

57. 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. This is necessary for the parties to be able to determine who is processing which personal data for whom and for what purpose, and what instructions are applicable and who is allowed to give instructions. Any ambiguity would make it impossible for controllers or processors to fulfil their obligations under the accountability principle.

58. Where the parties providing or using certain processing services, the description (details) of the processing, the applicable technical and organizational measures, the instructions from the controller concerning the processing of personal data, the specific restrictions and/or additional safeguards concerning data of special category, the authorized sub-processors, and/or the technical and organisational measures by which the processor is required to assist the controller differ, the parties should be required to complete further Annexes I to VII, unless the differences are very limited and the exceptions clearly described in the Annexes.

59. In the case of a complex contract, which for example comprises several parties or several purposes, it must always be clear which Annex (or in case of limited deviations in one single Annex: which stipulation of such Annex) applies to which specific situation or relation. It is necessary to clearly identify and distinguish the different processing activities.
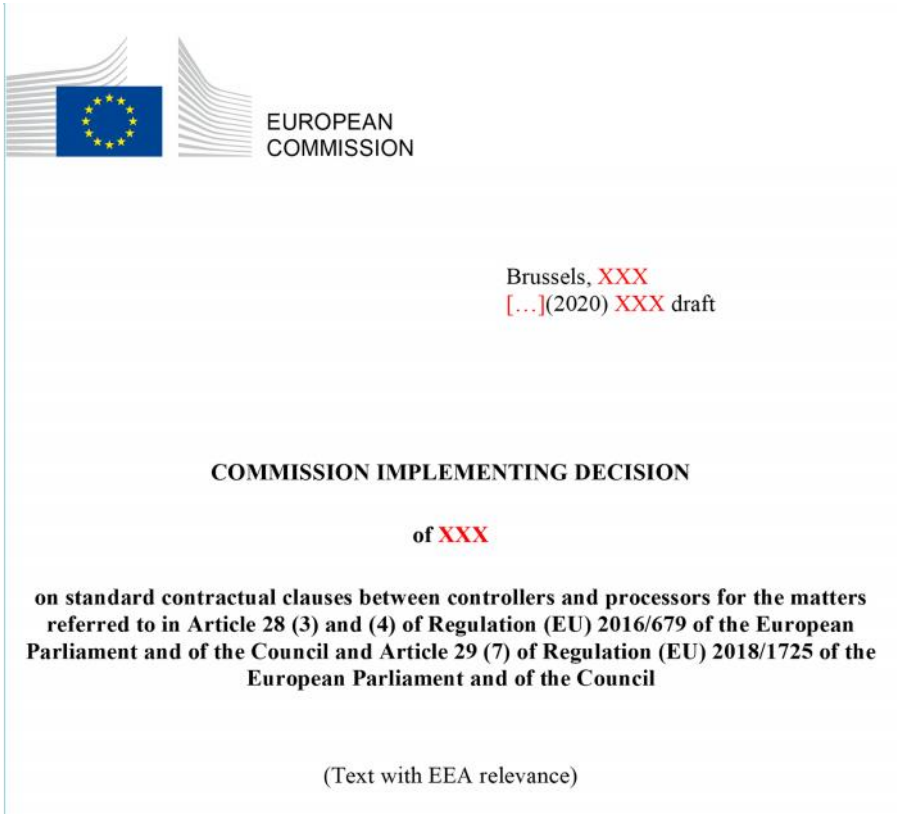
***

For the European Data Protection Supervisor   For the European Data Protection Board

The European Data Protection Supervisor   The Chair

(Wojciech Wiewiorowski)   (Andrea Jelinek)

EUROPEAN COMMISSION

Brussels, XXX
[…](2020) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

(Text with EEA relevance)

Commented [A1]: The title is referring to 28 (3) - (4) GDPR on one side and 29 (7) EUDPR on the other side. We should align and either refer to 28(3) and (4) GDPR / 29 (3) and (4) EUDPR or to 28 (7) GDPR / 29 (7) EUDPR.

Also the title is not aligned with the one mentioned in the Annex

Annex 1 to the EDPB - EDPS Joint Opinion 1/2021 - Comments and suggested changes to the Draft Implementing Decision

COMMISSION IMPLEMENTING DECISION

of XXX

on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 repealing Directive 95/46/EC (GDPR)[1], and in particular Article 28(7) thereof,

Having regard to 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (EUDPR)[2], and in particular Article 29(7) thereof,

Whereas:

(1)   The concepts of controller and processor play a crucial role in the application of Regulation (EU) 2016/679 and of Regulation (EU) 2018/1725. The controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purpose of Regulation (EU) 2018/1725, a controller means the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by the Union. A processor is the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

> **Commented [A2]:** We suggest adding "by Union law" as per the definition of controller under Article 3(8) EUDPR

(2)   The same set of standard contractual clauses should apply in respect of the relationship between data controllers and data processors subject to Regulation (EU) 2016/679 and Regulation (EU) 2018/1725, respectively. This is justified by the fact that, in the interest of a coherent approach to personal data protection throughout the Union and the free movement of personal data within the Union the data protection rules applicable to the public sector in the Member States and the data protection rules for Union institutions, bodies, offices and agencies were aligned as far as possible between Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

> **Commented [A3]:** These definitions do not exist in the law. We would rather suggest to refer to the notions of "controller" and "processor".

---

[1]   OJ L 119, 4.5.2016, p. 1.
[2]   OJ L 295, 21.11.2018, p. 39.

(3)   To ensure compliance with the requirements of Regulations (EU) 2016/679 and (EU) 2018/1725, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures which meet the requirements of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 , including for the security of processing.

(4)   The processing by a processor is to be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the elements listed in Article 28(3) and (4) of Regulation (EU) 2016/679 or Article 29(3) and (4) of Regulation (EU) 2018/1725. That contract or act is in writing, including in electronic form.

(5)   In accordance with Article 28(6) of Regulation (EU) 2016/679 and Article 29(6) of Regulation (EU) 2018/1725, the controller and the processor may choose either to negotiate an individual contract containing the compulsory elements laid down in Article 28(3) and (4) of Regulation (EU) 2016/679 or Article 29(3) and (4) of Regulation (EU) 2018/1725, respectively, or to rely, in whole or in part, on standard contractual clauses adopted by the Commission pursuant to Article 28(7) of Regulation (EU) 2016/679 and Article 29(7)of Regulation (EU) 2018/1725.

> **Commented [A4]:** We would suggest to explain further to which extent parties can rely only in part on SCCs and to clarify that in case SCCs are relied upon only in part, the requirements of Article 28 (3) and (4) GDPR should still be fulfilled.

(6)   The controller and processor should be free to include the standard contractual clauses laid down in this Decision 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. Reliance on the standard contractual clauses is notwithstanding any contractual obligations of the controller and or processor to ensure respect for applicable privileges and immunities..

> **Commented [A5]:** We suggest to clarify that this sentence and this reference to applicable privileges and immunities is relevant in the framework of SCCs under Regulation 2018/1725.

(7)   The standard contractual clauses should provide for both substantive and procedural rules. Moreover, in line with Article 28(3) of Regulation (EU) 2016/679 and Article 29(3) of Regulation (EU) 2018/1725, the standard contractual clauses should require the controller and processor to set out the subject matter and duration of the processing, its nature and purpose, the type of personal data concerned, as well as the categories of data subjects and the obligations and rights of the controller.

(8)   Pursuant to Article 28(3) of Regulation (EU) 2016/679 and pursuant to Article 29(3) Regulation (EU) 2018/1725, the processor has to inform the controller immediately, if, in its opinion, an instruction of the controller infringes Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, respectively or other Union or Member State data protection provisions.

(9)   Where a processor engages another processor for carrying out specific activities, the specific requirements referred to in Article 28(2) and (4) of Regulation (EU) 2016/679 or Article 29(2) and (4) of Regulation (EU) 2018/1725 should apply. In particular, a prior written authorisation is required. Such authorisation could be specific or general. In both cases, the first processor should keep a list of other processors updated.

> **Commented [A6]:** We suggest including "prior written authorisation of the controller" to make it explicit that in line with the GDPR and EUDPR this is always the prior authorisation of the controller.

> **Commented [A7]:** We would suggest to use the wording "initial processor" in line with the terminology in GDPR and EUDPR. Moreover, where a reference is made to the "list of other processors", it should be clear that it refers also to sub-processor.

(10)   To fulfil the requirements of Article 46(1) Regulation (EU) 2016/679, the Commission adopted standard contractual clauses pursuant to Article 46(2)(c) Regulation (EU) 2016/679. Those clauses also fulfil the requirements of Article 28(3) and (4) of Regulation (EU) 2016/679 for data transfers from controllers subject to Regulation (EU) 2016/679 to processors outside the territorial scope of application of that Regulation or

> **Commented [A8]:** See comment in the Joint Opinion on the scope and interaction with the transfer SCCS.

from processors subject to Regulation (EU) 2016/679 to sub-processors outside the territorial scope of that Regulation.

(11) Third parties should be able to become a party to the standard contractual clauses throughout the life cycle of the contract.

(12) The operation of the standard contractual clauses should be evaluated in the light of experience, as sub-part of the periodic evaluation of Regulation (EU) 2016/679 referred to in Article 97 of that Regulation.

(13) [PLACEHOLDER: The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered a [joint opinion] on […]³, which has been taken into consideration in the preparation of this Decision.]

(14) [PLACEHOLDER: The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679 and Article 96(2) of Regulation (EU) 2018/1725.

HAS ADOPTED THIS DECISION:

Article 1

The standard contractual clauses as set out in the Annex fulfil the requirements for contracts between the controller and the processor in Article 28(3) and (4) of Regulation (EU) 2016/679 and of Article 29(3) and (4) of Regulation (EU) 2018/1725.

Article 2

The standard contractual clauses as set out in the Annex may be used in contracts between a controller and a processor who processes personal data on its behalf, where the controller and the processor are subject to Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 .

Article 3

The Commission shall evaluate the practical application of the standard contractual clauses set out in the Annex on the basis of all available information as part of the periodic evaluation provided for in Article 97 of Regulation (EU) 2016/679.

Article 4

This Decision shall apply from …

Done at Brussels,

For the Commission
Ursula VON DER LEYEN
The President

---

³

Commented [A9]: In terms of wording, we would prefer referring to the "implementation of the use of SCCs" or "practical application" as mentioned in Art. 3 below.

Commented [A10]: We would also recommend to add a reference to the review process of Art. 97 EUDPR.

Commented [A11]: See comment in the text of the Joint Opinion.

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

EN **EN**

<u>**ANNEX**</u>

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.

EN

2

EN

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

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

(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].

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.

7.2. Erasure or return of data

Processing by the data processor shall only take place for the duration specified in Annex II.

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

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

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.

[OPTION 1] delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so /

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

[OPTION 2] return all the personal data to the data controller

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

and delete existing copies unless Union or Member State law requires storage of the personal data.

7.3. Security of processing

(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 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)   tThe 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(cb) 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:

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

(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;

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

(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:

> **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.

(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 [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

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.

…

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

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]

[DESCRIBE REQUIREMENTS FOR DATA QUALITY]

[DESCRIBE REQUIREMENTS FOR DATA RETENTION]

[DESCRIBE REQUIREMENTS FOR ACCOUNTABILITY]

[DESCRIBE REQUIREMENTS FOR DATA PORTABILITY AND DATA DISPOSAL]

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.

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.

EDPB - EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries

for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679

TABLE OF CONTENTS

The European Data Protection Board and the European Data Protection Supervisor

Having regard to Article 42(2) of the Regulation 2018/1725 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

HAVE ADOPTED THE FOLLOWING JOINT OPINION

1   BACKGROUND

1. In compliance with Article 44 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[2] ("**GDPR**"), any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in Chapter V GDPR are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. In particular, in the absence of an adequacy decision, any transfer should be based on appropriate safeguards listed in Article 46 GDPR.

2. Standard data protection clauses adopted by the European Commission (or the "**Commission**") in accordance with the examination procedure referred to in Article 93(2) GDPR ("**SCCs**") are one of the appropriate safeguards listed by Article 46 GDPR.

3. In order to be valid, SCCs must incorporate effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to these clauses are suspended or prohibited in the event of the breach of such clauses or if it is impossible to honour them[3].

---

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

[2] 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 repealing Directive 95/46/EC (General Data Protection Regulation); OJ L 119, 04.05.2016, p. 1–88.

[3] Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems; Case C-311/18; para 137.

4.   On 15 June 2001, the Commission adopted Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [4], as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 [5] ("**the 2001 SCCs**"), complemented by Commission Decision of 27 December 2004 [6] ("**the 2004 SCCs**").

5.   On 5 February 2010, the Commission adopted Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC [7], later amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 [8] ("**the 2010 SCCs**").

6.   On 16 July 2020, the Court of Justice of the EU ("**CJEU**" or "**the Court**") ruled that the examination of the 2010 SCCs in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights disclosed nothing to affect the validity of that decision ("**the Schrems II ruling**") [9].

7.   In the same case, the CJEU also provided for additional clarifications on the use of SCCs. In particular, the CJEU ruled that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses should be afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union [10].

8.   The CJEU added that *"[s]ince by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries [...] it may prove necessary to supplement the guarantees contained in those standard data protection clauses."* [11].

---

[4] 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; OJ L 181, 04.07.2001, p. 19-31.

[5] Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council; OJ L 344, 17.12.2016, p. 100–101.

[6] 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries; OJ L 385, 29.12.2004, p. 74–84.

[7] 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council; OJ L 39, 12.2.2010, p. 5–18.

[8] Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council; OJ L 344, 17.12.2016, p. 100–101.

[9] Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems; Case C-311/18; para 149.

[10] Ibid, para 96

[11] Ibid, para 132

9.   Consequently, on 10 November 2020, the EDPB adopted its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ("**the EDPB Recommendations on supplementary measures**")[12].

10.   On 12 November 2020, the Commission published:

   ➢ A draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**the Draft Decision**"); and

   ➢ A draft Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**the Draft SCCs**").

11.   The Draft Decision plans to repeal the 2001, 2004 and 2010 SCCs.

12.   The Draft SCCs combine general clauses with a modular approach to cater for various transfer scenarios. In addition to the general clauses, controllers and processors should select the module applicable to their situation among the four following modules:

   ➢ Module One: transfer controller to controller;

   ➢ Module Two: transfer controller to processor;

   ➢ Module Three: transfer processor to processor;

   ➢ Module Four: transfer processor to controller.

13.   In this context, on 12 November 2020, the Commission requested the EDPB and the EDPS to issue a Joint Opinion on the Draft Decision and the Draft SCCs ("**the Joint Opinion**"), in compliance with Article 42(2) 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 ("**EUDPR**")[13].

2   GENERAL REASONING REGARDING THE DRAFT DECISION AND THE DRAFT SCCs

2.1   General structure and methodology of the Joint Opinion

14.   **First,** for the sake of clarity, the Joint Opinion comprises (i) a core part detailing general comments the EDPB and the EDPS wish to make and (ii) an annex where additional comments of a more technical nature are made directly to the Draft SCCs, notably in order to provide some examples of possible amendments. There is no hierarchy between the general comments and the technical ones.

---

[12] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymea surestransferstools_en.pdf.

[13] 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC; OJ L 295, 21.11.2018, p. 39–98.

15. **Second,** the general comments on the Draft Decision and the Draft SCCs are presented in two separate sections. Where needed, cross-references are made to ensure consistency.

16. **Third,** for the sake of consistency, where needed, cross-references are also made to the Joint Opinion of the EDPB and the EDPS on standard contractual clauses between controllers and processors under Article 28(7) GDPR and Article 29(7) EUDPR.

2.2 General presentation of the Draft Decision and Draft SCCs and interplay with the EDPB Recommendations on supplementary measures

17. Overall, the EDPB and the EDPS note with satisfaction that the Draft Decision and the Draft SCCs present a reinforced level of protection for data subjects.

18. Following up on the EDPB contribution for the evaluation of the GDPR under Article 97 GDPR[14], the EDPB and the EDPS welcome the fact that this update of existing SCCs intends to:

   ➢ Bring the SCCs in line with new GDPR requirements[15].

   ➢ Better reflect the widespread use of new and more complex processing operations often involving multiple data importers and data exporters, long and complex processing chains, as well as evolving business relationships. This means covering additional processing and transfer situations and using a more flexible approach, for example with respect to the number of parties able to join the contract[16].

   ➢ Provide for specific safeguards to address the effect of the laws of the third country of destination on the data importer's compliance with the clauses, and in particular how to deal with binding requests from public authorities in the third country for disclosure of the personal data transferred[17].

19. In particular, the EDPB and the EDPS welcome the specific provisions intending to address some of the main issues identified in the Schrems II ruling, and in particular the provisions of the Draft SCCs on:

   ➢ Third country's laws affecting compliance with the Draft SCCs (Section II - Clause 2);

   ➢ Access requests received by the data importer and issued by third country's public authorities (Section II - Clause 3); and

   ➢ Optional ad-hoc redress mechanism to the benefit of data subjects (Section II - Clause 6).

20. In addition, the EDPB and the EDPS note with satisfaction that the Draft SCCs reflect several measures identified in the EDPB Recommendations on supplementary measures, although for some others the EDPB and the EDPS call for more consistency, as notably detailed in Section 4.3.6 below.

21. In this context, the EDPB and the EDPS recall that the EDPB Recommendations on supplementary measures will remain relevant to be applied after the adoption of the Draft SCCs. In particular, the

---

[14] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.
[15] Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; Recital 6.
[16] Ibid, Recital 6.
[17] Ibid, Recital 18.

EDPB and the EDPS call on the Commission to clarify that there may still be situations where, despite the use of the new SCCs, ad-hoc supplementary measures will remain necessary to be implemented in order to ensure that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU. As such, the new SCCs will have to be used along with the EDPB Recommendations on supplementary measures. The EDPB and the EDPS invite the European Commission to refer to the final version of the EDPB Recommendations on supplementary measures, should the final version of the Recommendations be updated before the Draft Decision and the Draft SCCs[18].

3   ANALYSIS OF THE DRAFT DECISION

3.1   References to the EUDPR (Recital (8))

22.   The EDPB and the EDPS take note that Recital (8) of the Draft Decision reads as follows:

"The standard contractual clauses may also be used for the transfer of personal data to a sub-processor in a third country by a processor that is not a Union institution or body, processing personal data on behalf of such an Union institution or body in accordance with Article 29 of Regulation (EU) 2018/1725 of the European Parliament and of the Council. Doing so will also ensure compliance with Article 29(4) of Regulation (EU) 2018/1725, to the extent these clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [....]".

23.   The EDPB and the EDPS understand that the intention of the Commission is that the Draft SCCs should cover processing operations between processors and sub-processors for which the controller is an EU institution, body, office or agency ("**EUI**") subject to the EUDPR.

24.   In this respect, the EDPB and the EDPS consider that the relevant requirements of the EUDPR should be reflected throughout the entire chain of contracts when a EUI is the controller. This should be further clarified in the Draft Decision and Draft SCCs.

25.   In any event, the EDPB and the EDPS recall that it remains always possible for the Commission to remove any reference to the EUDPR if it decides not to apply the draft Article 46 SCCs to relations between processors and sub-processors being part of a processing operation for which the controller is a EUI subject to the EUDPR.

3.2   The scope of the Draft Decision and the notion of transfers (Article 1(1))

26.   **First,** Article 1(1) of the Draft Decision provides that:

*"The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer of personal data from a controller or processor subject to Regulation (EU) 2016/679 (data exporter) **to a controller or (sub-) processor not subject to Regulation (EU) 2016/679 (data importer)."***

18

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasu restransferstools_en.pdf. This document was submitted for public consultation until 21 December 2020 and is still subject to possible further modifications on the basis of the results of the public consultation.

27. In view of the above and of the title the Draft Decision, the EDPB and the EDPS understand that the Draft Decision does not cover:

> ➤ Transfers to a data importer not in the EEA but subject to the GDPR for a given processing under Article 3(2) GDPR; and

> ➤ Transfers to international organisations.

28. Keeping this in mind, for the avoidance of doubt, the EDPB and the EDPS recommend the Commission to clarify that these provisions are only intended to address the issue of the scope of the Draft Decision and the draft SCCs themselves, and not the scope of the notion of transfers.

29. **Second,** the EDPB already clarified in its Guidelines on the territorial scope of the GDPR [19] that a controller or processor is never subject as such to the GDPR, but only in relation to a given processing activity.

30. Therefore, the EDPB and the EDPS recommend rephrasing Article 1(1) of the Draft Decision accordingly.

4 ANALYSIS OF THE DRAFT SCCs

4.1 General remark on the Draft SCCs

31. The EDPB and the EDPS welcome the introduction of specific modules for each transfer scenarios. However, the EDPB and the EDPS note that it is not clear whether one set of the SCCs can include several modules in practice to address different situations, or whether this should amount to the signing of several sets of the SCCs. In order to achieve maximum readability and easiness in the practical application of the SCCs, the EDPB and the EDPS suggest that the European Commission provides additional guidance (e.g. in the form of flowcharts, publication of Frequently Asked Questions (FAQs), etc.). In particular, it should be made clear that the combination of different modules in a single set of SCCs cannot lead to the blurring of roles and responsibilities among the parties.

4.2 Section I

4.2.1 Clause 1 - Purpose and scope

32. In relation to the reference to standard contractual clauses pursuant to Article 28(7) GDPR included in Clause 1(c), the EDPB and the EDPS consider that it is important to clearly explain in the Draft Decision, the articulation and interplay between this set of SCCs and the SCCs pursuant to Article 28(7) GDPR. It should be made clear to the parties, already in the Draft Decision, that when parties intend to benefit from SCCs both under Article 28(7) and Article 46(2)(c) GDPR, then the parties need to rely on transfer SCCs. According to Clause 1(c) of the Draft SCCs, the parties are allowed to add other clauses or additional safeguards *"provided that they do not contradict, directly or indirectly,"* the Draft SCCs. To provide controllers and processors with legal certainty, the EDPB and the EDPS would welcome clarifications on the type of clauses that the European Commission would consider as contradicting directly or indirectly the Draft SCCs. Such clarification could, for instance, indicate that clauses contradicting the Draft SCCs would be those that undermine / negatively impact the obligations in the Draft SCCs or prevent compliance with the obligations contained in the Draft SCCs. For example,

---

clauses allowing processors to use the data for their own purposes would be contrary to the obligation of the processor to process personal data only on behalf of the controller and for the purposes and by the means identified by the latter.

4.2.2   Clause 2 - Third party beneficiaries

33.   Pursuant to Section, I Clause 2, "*Data subjects may invoke and enforce these Clauses, as third party beneficiaries".* However, this right solely applies to the provisions that are <u>not</u> listed under this Clause 2. For the sake of providing clear and unambiguous information to data subjects on their rights, as well as to controllers and processors that will use the Clauses on those third party beneficiary rights, the EDPB and the EDPS invite the European Commission to provide, under this Clause 2, a 'positive' list of the rights that are enforceable by data subjects, instead of listing those that are not enforceable[20].

34.   In terms of substance, the EDPB and the EDPS note that a number of the provisions included in the list provided in Clause 2 should actually be made enforceable by data subjects, hence should be deleted from that list.

35.   The EDPB and the EDPS are of the view that, as this is currently the case in the previous sets of SCCs adopted by the European Commission[21], and as it is required by SAs for binding corporate rules ("**BCRs**"), **Section I Clause 2 (Third party beneficiaries)** itself should be subject to enforceability by data subjects.

36.   Concerning **Section I, Clauses 3 (Interpretation) and 4 (Hierarchy)**, it should be noted that if the parties do not respect the rules on interpretation and on the hierarchy of documents, it may have an impact on data subjects and their rights. Therefore, the EDPB and the EDPS believe that this Clause should be made enforceable by data subjects.

37.   Under **Section II, Module Two: Clause 1.9(a) and Module Three: Clause 1.9(a)** contain the same requirements. They cover the data importer's obligation to deal with the data exporter's inquiries (as well as the controller's inquiries, for Module Three). If breached, the EDPB and the EDPS are of the view that these two Clauses may have an impact on data subjects and their rights, hence should be deemed enforceable by data subjects, as this is currently the case in the previous sets of SCCs adopted by the European Commission[22].

38.   Under Section II, Module Three: Clause 1.1(a) relates to the data exporter's obligation to inform the data importer that it acts under the controller's instructions; Clause 1.1(b) sets out the data importer's obligation to process the personal data under the controller's instructions and those transmitted by the data exporter; and Clause 1.1(c) relates to the data importer's obligation to inform the data exporter when the data importer is unable to follow those instructions and the data exporter's obligation to notify it to the controller. The EDPB and the EDPS note that a breach of **Section II, Module Three: Clause 1.1(a), (b), and (c)** may have an impact on data subjects and their rights, hence should

---

[20] This would be better aligned with the way Chapter III GDPR is drafted, as well as with the previous sets of SCCs adopted by the European Commission (see Clause 3 2001 SCCs; Clause III(b) 2004 SCCs; and Clause 3.1 2010 SCCs).

[21] See Clause 3 in 2001 SCCs; Clause III(b) in 2004 SCCs; Clause 3 in 2010 SCCs.

[22] See Clause 5(e) in 2010 SCCs.

be made enforceable by them, as this is currently the case in the previous sets of SCCs adopted by the European Commission[23].

39. Under **Section II, Module Four: Clause 1.1**, the EDPB and the EDPS note that Clause 1.1(a) and (b) relate to the data exporter's obligation, respectively to process the data under the data importer's instructions and to inform the data importer if the data exporter is unable to comply with the controller's instructions or if they infringe Union or Member State's data protection law; and Clause 1.1(c) covers the data importer's obligation to refrain from taking any action preventing the data exporter from fulfilling its obligations under GDPR. **Section II, Module Four: Clause 1.3** touches upon the parties' ability to demonstrate compliance with their commitments taken under the SCCs.

40. Given that a breach of the commitments set out under **Section II, Module Four: Clause 1.1(a), (b), and (c), and Clause 1.3** may have an impact on data subjects and their rights, they should be made enforceable by data subjects.

41. The EDPB and the EDPS note that non-compliance with sub-processing commitments may have an impact on data subjects and their rights, thus **Section II, Clause 4(a), (b), and (c)** should be made enforceable by data subjects, as this is currently the case in the previous sets of SCCs adopted by the European Commission[24].

42. The EDPB and the EDPS note that **Section II, Clause 9(b)** deals with the data importer's agreement to cooperate with the competent supervision authority. As a breach of this commitment may have an impact on data subjects and their rights, the EDPB and the EDPS consider that it should be made enforceable by data subjects, as this is currently the case in the previous sets of SCCs adopted by the European Commission[25], as well as in BCRs[26].

43. The EDPB and the EDPS note that, **Section III, Clause 1(a)** provides for the obligation on the data importer to inform the data exporter if it cannot comply with the SCCs, from which follows the obligation for the data exporter to suspend the transfer(s) (Clause 1(b)), which may then terminate the contract upon certain conditions (Clause 1(c)) and instruct the data importer on what happens to the data after such termination (Clause 1(d)).

44. Since these provisions touch upon situations where the data importer cannot comply with the SCCs and/or is in breach of the SCCs, the EDPB and the EDPS are of the view that a violation of **Section III, Clause 1(a), (b), (c), and (d)** may have an impact on data subjects and their rights, and should therefore

---

[23] This comment only applies for Section II Module Three: Clause 1.1(b) (see Clause 5(a) in 2010 SCCs) and Clause 1.1(c) (see Clause 5(b) in 2010 SCCs) of the Draft SCCs. There is no equivalent of Section II Module Three: Clause 1.1(a) in the previous SCCs.

[24] See Clause 5(h)(i) and (j) in 2010 SCCs.

[25] See Clause 5(c) in 2001 SCCs; Clause II(e) in 2004 SCCs; Clause 8.2 in 2010 SCCS.

[26] See Article 47(2)(l) GDPR. See also Section 3.1 of the Working Document setting up a table with the elements and principles to be found in BCRs (WP256 rev.01), adopted by the Article 29 Working Party and endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109; and Section 3.1 of the Working Document setting up a table with the elements and principles to be found in Processor BCRs (WP257 rev.01), adopted by the Article 29 Working Party and endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

be able to enforce them, as this is currently the case in the previous sets of SCCs adopted by the European Commission[27], as well as in BCRs[28].

4.2.3 Clause 6 - Docking clause

45.   The EDPB and the EDPS welcome the inclusion of a docking clause in Clause 6, which allows, as an option, any entity to accede to the Draft SCCs and therefore to become a new party to the contract as a controller or as a processor. The qualification and the role of the parties to the contract should appear clearly in the Annexes, especially in the case where new parties accede to the contract. Thus, the Annex should detail and delimit the allocation of responsibilities, and indicate clearly which processing is carried out by which processor(s) on behalf of which controller(s), and for which purposes.

46.   Clause 6(a) makes the accession of new parties to the Draft SCCs conditional upon the agreement of all the other parties. In order to avoid any difficulties in practice, the EDPB and the EDPS would welcome a clarification on the way such agreement could be given by the other parties (e.g. whether it has to be provided in writing, the deadline, the information needed before agreeing). Moreover, the EDPB and the EDPS would welcome clarification as to whether and how such agreement has to be given by all the parties, irrespective of their qualification and role in the processing.

4.3   Section II - Obligations of the parties

4.3.1   Clause 1 - Data protection safeguards – Module One (Transfer controller to controller)

4.3.1.1   Scope of Module One (Transfer controller to controller)

47.   This module seems to cover transfers between controllers acting as independent or separate controllers. In order to avoid any ambiguity, the EDPB and the EDPS call on the Commission to assess and clarify, in the Draft Decision or in the Draft SCCs, if this module is only relevant for independent or separate controllers, or if it could also be used in joint controllership scenarios with regard to processing of personal data carried out by joint-controllers where one of the joint controller is established outside of the EU and not subject the GDPR.

4.3.1.2   Clause 1.2 - Transparency

48.   Clause 1.2(a) of the Draft SCCs lists the elements on which the data importer must provide information to data subjects whose personal data are transferred. To ensure full transparency and put data subjects in a position to exercise their rights as provided by this clause, the EDPB and the EDPS consider that the list of elements should further be completed, so as to be brought in line with Article 14(1) and (2) GDPR relating to indirect collection of data. As such, this clause should be complemented with information on the types of personal data processed by the data importer, and the period for which personal data will be stored by the latter (or criteria used to determine it).

49.   In addition, this clause should specify the timing in which the data importer shall provide this information to data subjects so as to meet the conditions set out by Article 14(3) GDPR.

---

[27] See Clause 5(a) in 2001 SCCs; Clause II(c) in 2004 SCCs; Clauses 5(a) and (b), and Clause 12.1 in 2010 SCCs.
[28] See Section 6.3 of the Working Document setting up a table with the elements and principles to be found in BCRs (WP256 rev.01); and Section 6.3 of the Working Document setting up a table with the elements and principles to be found in Processor BCRs (WP257 rev.01).

50. Furthermore, it results from Clause 1.2(b) that the data importer may be exempted from providing information to data subjects in accordance with Clause 1.2(a), notably where providing such information proves impossible or would involve a disproportionate effort in which case the data importer shall, to the extent possible, make the information publicly available. The use of the term "*to the extent possible*" does not appear in line with Article 14(5)(b) GDPR and should be deleted. Indeed, Article 14(5)(b) GDPR does not provide for such condition but rather sets a clear requirement that information is made publicly available to the data subject where providing such information proves impossible or would involve a disproportionate without any possible derogation.

4.3.1.3   Clause 1.5 - Security of processing

51. In connection with the data importer's obligation to implement appropriate measures to ensure the security of transferred data, Clause 1.5(a) specifies that the parties shall consider "*encryption during transmission and anonymisation or pseudonymisation, where this does not prevent fulfilling the purpose of processing".* In relation to the reference to anonymization, the EDPB and the EDPS recall that if personal data are anonymized, the obligations under the GDPR are no longer applicable.

4.3.1.4   Clause 1.7 - Onward transfers

52. The obligations of the data importer under this clause raise several issues:

53. First of all, the EDPB and the EDPS note that this clause does not include a commitment from the data importer to notify the data exporter of the existence of an onward transfer as is the case in the 2004 SCCs for transfers from controllers to controllers. The EDPB and the EDPS do not see the reason for not replicating this obligation in the proposed Draft SCCs. Such information of the data exporter is essential to allow the latter to comply with its obligations under Article 44 GDPR, which specifically refer to onward transfers and ensure accountability, as required by the GDPR, for any processing in this specific case for the processing subject to the onward transfer.

54. Further, Clause 1.7 provides that the data importer may carry out an onward transfer if the third party is or agrees to be bound by the Draft SCCs. It is unclear however, how this provision would work in practice if the third party concerned is a processor, notably how it would be bound by the clauses, which requirements will apply to it, and whether the parties could add another module (i.e. Module Two) that would be relevant for that situation. This point requires clarification in the Draft SCCs to avoid any confusion in practice, and ensure legal certainty for the parties. In addition, it should be made clear that the third party should assess whether it is able to comply with the obligations set out by the Draft SCCs under the third country law applicable to this third party and, where necessary, to implement supplementary measures to ensure a level of protection essentially equivalent to the one required in the EEA.

55. In addition, Clause 1.7(iii) specifies, amongst other conditions, that an onward transfer may be allowed where the data importer and the third party enter into an agreement ensuring "*the same level of data protection*" as under the Draft SCCs. According to the EDPB and the EDPS, the reference to the "*same level of data protection*" does not appear sufficient as the agreement needs to replicate in substance the same guarantees and obligations as those contained in the Draft SCCs to ensure the continuity of the protection in line with Article 44 GDPR. This clause should be amended accordingly, by stating that the agreement must impose the same obligations as those included in the Draft SCCs between the data exporter and the data importer. In addition, a specific obligation shall be added in this case for the parties to assess whether they are able to comply with the obligations set out by such agreement under the third country law applicable to this third party, and, where necessary, to implement supplementary measures to ensure a level of protection essentially equivalent to the one required in the EEA.

56.   Furthermore, an obligation should be added for the data importer to provide data subjects with a copy of the safeguards implemented for the onward transfer, upon request. The provision of a copy of such safeguards to data subjects contributes to the transparency which is required in relation to the transfer of their data.

57.   Finally, Clause 1.7(iv) sets out that an onward transfer could be carried out where the data importer has obtained the explicit consent of the data subject. The possibility of relying on the data subject's consent corresponds to the derogation for specific situations envisaged by Article 49(1)(a) GDPR. The EDPB and the EDPS are of the opinion that the derogatory and exceptional nature of this possibility needs to be stated in the Draft SCCs, in particular compared to other possibilities for framing onward transfers referred in this clause. As such, it must be specified that the consent of the data subject could, as an exception, frame the onward transfers only if other mechanisms listed in Clause 1.7 cannot be relied upon. Also, the EDPB and the EDPS are of the opinion that the Commission should assess the possibility of onward transfers in particular for the establishment, exercise or defence of legal claims, and to protect the vital interests of the data subject or of other persons.

4.3.2   Clause 1 - Data protection safeguards – Module Two (Transfer controller to processor)

4.3.2.1   Clause 1.5 - Storage limitation and erasure or return of the data

58.   Clause 1.5 of the Draft SCCs stipulates that upon termination of the provision of the processing services, the data importer shall delete all personal data processed on behalf of the data exporter (option 1) or return to the data exporter all personal data processed on its behalf, and delete existing copies (option 2). The EDPB and the EDPS are of the opinion that this wording conflicts with Article 28(3)(g) GDPR, which provides for that deletion or returning takes place "*at the choice of the controller*". Accordingly, Clause 1.5 should provide for that deletion or returning of personal data to take place at the choice of the data exporter acting as a controller to avoid any ambiguity that such choice is not up to the data importer acting as a processor.

59.   In addition, this clause provides that in case the data importer does not delete or return the data to the data exporter due to local requirements applicable to the data importer, it will guarantee the level of protection required by the Draft SCCs "*to the extent possible*". The EDPB and the EDPS consider that if data are to be kept by the data importer, the protection provided by the Draft SCCs needs to be fully ensured and without exceptions, to allow for the continuity of the protection. As a consequence, the terms "*to the extent possible*" should be deleted from this clause.

60.   Moreover, Clause 1.5 sets forth that the data importer's obligation to return or delete the personal data is notwithstanding any requirements "*under local law*" which prohibits return or destruction. This wording amounts to contradicting Article 28(3)(g) GDPR. The Commission should clarify in the Draft SCCs that only the requirements of local 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 should be taken into account under this clause. The EDPB and the EDPS consider that specific legal requirements in terms of data retention periods under local laws, types of data, and retention periods should be explicitly specified under Annex I.B.

4.3.2.2   Clause 1.6 - Security of processing

61.   Similarly as in Module One, Clause 1.6(a) specifies that in order to ensure the security of data as part of the transfer, the parties shall consider "*encryption during transmission and anonymisation or pseudonymisation, where this does not prevent fulfilling the purpose of processing".* In relation to the reference to anonymization, the EDPB and the EDPS recall that if personal data is anonymized, the obligations under the GDPR are no longer applicable.

62.   Furthermore, Clause 1.6(d) provides for the data importer's obligation to cooperate "*in good faith*" and assist the data exporter to comply with its obligations under the GDPR. The terms "*in good faith*" are not used in other parts of the SCCs where an obligation of cooperation is mentioned and the EDPB and the EDPS do not see the need for such specification, which, in any case, would go beyond the provisions of the GDPR on that matter. It should thus be deleted.

4.3.2.3   Clause 1.8 - Onward transfers

63.   Clause 1.8(i) should be completed with an obligation for the data importer to provide the data exporter, upon request, with a copy of the safeguards implemented for framing onward transfers to a third party. Such obligation was included in the controller to processor 2010 SCCs. The EDPB and the EDPS do not see the reason for its exclusion from the proposed Draft SCCs, as the provision of these safeguards constitute an important element for the data exporter's obligation under GDPR to ensure accountability with respect to the transfers it carries out, including onward transfers.

64.   An obligation should also be added for the data importer to provide data subjects with a copy of these safeguards upon request, as is the case in the controller to processor 2010 SCCs. As above, the EDPB and the EDPS do not see the reason for excluding such obligation from the proposed Draft SCCs. The provision of these safeguards to the data subject contribute to the transparency which is required in relation to the transfer of their data.

4.3.2.4   Clause 1.9 - Documentation and compliance

65.   **Clause 1.9(d)** of the Draft SCCs provides for the possibility for the data exporter, in order to conduct audits, to rely on an independent auditor mandated by the data importer. This provision is not foreseen in Article 28(3)(h) GDPR, and needs to be aligned with this article which provides that the processor has to allow for and contribute to audits, including inspections, that are conducted by the controller or another auditor mandated by the controller[29]. As such, the processor might propose an auditor, but the decision about the auditor has to be left to the controller according to Article 28(3)(h) GDPR. The controller's right to choose the auditor should not be limited from the outset. Clause 1.9(d) also states that where the data exporter mandates an independent auditor, it shall bear the costs, and where the data importer mandates an audit, it has to bear the costs of the independent auditor. As the issue of allocation of costs between a controller and a processor is not regulated by the GDPR, consequently, the EDPB and the EDPS are of the opinion that any reference to the costs should be deleted from this clause. The same comment applies to the corresponding provision in Module Three.

---

[29] As this is currently required by the EDPB in the context of BCRs for processors, see WP257 (endorsed by the EDPB), Section 2.3 "*Any processor or sub-processor processing the personal data on behalf of a particular controller will accept, at the request of that controller, to submit their data processing facilities for audit of the processing activities relating to that controller which shall be carried out by the controller or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the data controller, where applicable, in agreement with the Supervisory Authority.";* https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49726 https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49726.

4.3.3 Clause 1 - Data protection safeguards – Module Three (Transfer processor to processor)

66. Pursuant to Clause 1.1, the data importer is obliged to process the personal data only based on the controller's instructions. In addition to that, Article 28(4) GDPR requires that, where a processor engages another (sub-)processor for carrying out specific processing activities on behalf of the controller, "*the same data protection obligations as set out in the contract or other legal act between the controller and the processor*" as referred to in Article 28(3) GDPR shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law. The EDPB and the EDPS are of the opinion that the requirement of Article 28(4) GDPR needs to be taken into account by the parties also in this scenario.

4.3.3.1   Clause 1.1 - Instructions

67. Module Three deals with processor to processor transfers. Accordingly, practitioners might initially assume that the contract pursuant to Article 46 GDPR may exclusively be concluded between the processor and its (sub-)processor if only Module Three is relied upon. However, Clause 1.1(a) refers to Annex I.A. and the list of "*parties*" which includes the identity and contact details of the controller and its signature. The EDPB and the EDPS are of the opinion that the Commission needs to clarify whether the controller has to sign these clauses, or whether the processor and sub-processor only need to mention the identity of the controller in the Annex. In the first case, it should be clarified to what effect and which obligations of Module Three would apply to the controller.

68. Furthermore, Clause 1.1 stipulates that the data exporter may give further instructions regarding the data processing "*within the framework of the contract agreed with the data importer throughout the duration of the contract*". It is not clear whether the reference to the framework of the contract limits in any way the controller's right to give further instructions regarding the data processing, all the more since Clause 7 of the draft Article 28 SCCs does not contain such possible limitation. Clause 7 states simply that "*Subsequent instructions may also be given by the data controller throughout the duration of the processing of personal data*".

4.3.3.2   Clause 1.5 - Storage limitation and erasure or return of data

69. Clause 1.5 stipulates that upon termination of the provision of the processing services, the data importer shall delete all personal data processed on behalf of the controller (option 1) or return to the data exporter all personal data processed on its behalf and delete existing copies (option 2). The EDPB and the EDPS are of the opinion that this wording conflicts with Article 28(3)(g) GDPR, which provides for that deletion or returning takes place "*at the choice of the controller*". Accordingly, Clause 1.5 should provide for that deletion or returning of personal data to take place at the choice of the controller. Furthermore, it should be added to option 2 that the data importer should be required to certify to the data exporter that it has deleted existing copies.

70. Apart from that, Clause 1.5 sets forth that the data importer's obligation to return or delete the personal data is notwithstanding any requirements "*under local law*" which prohibits return or destruction. This wording amounts to contradicting Article 28(3)(g) GDPR. Taking into account that the processor is subject to third country laws, and therefore may be subject to a legal obligation to (further) storage of the data (e.g. for accounting purposes), the EDPB and the EDPS consider that the Commission should clarify in the Draft SCCs that only the requirements of local 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 should be taken into account under this Clause. As in Module Two, the EDPB and the EDPS consider

that specific legal requirements in terms of data retention periods under local laws, types of data, and retention periods should be explicitly specified under Annex I.B.

Furthermore, the term "*to the extent possible*" should be deleted. To avoid repetition, the EDPB and the EDPS invite the Commission to refer to Section 4.3.2.1.

4.3.3.3   Clause 1.5 - Security of processing and Clause 1.6 - Special categories of personal data

71.   For the avoidance of repetition, the EDPB and the EDPS invite the Commission to refer to their comments made under Section 4.3.2.2.

4.3.4   Clause 1 - Data protection safeguards – Module Four (Transfer processor to controller)

72.   The EDPB and the EDPS recognise that the scope of Module Four includes only transfers from a processor subject to GDPR to its own controller not subject to GDPR, and excludes transfers from such a processor to any other controller, as is clarified in Article 1.1 and Recital 16 of the Draft Decision. Nevertheless, to avoid any misunderstanding about the scope of this module, the EDPB and the EDPS would recommend a short explanation of the limited scope of Module Four in the Draft SCC themselves.

73.   The EDPB and the EDPS would welcome any additional explanation that the European Commission could add in the Draft Decision regarding Module Four, so as to better understand the rationale used to determine which commitments shall be taken by parties using Module Four.

74.   To provide for all the necessary provisions of Article 28 GDPR directly applicable to the processor, Module Four should be completed as follows:

75.   There should be a commitment from the processor that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Article 28(3)(b) GDPR).

76.   A clause on the personal data breach notifications obligations imposed on the processor by virtue of Article 33(2) GDPR should also be added to this Module of the SCCs.

77.   Furthermore the Module should be completed with a clause on sub-processing by the processor/data exporter as this is a direct obligation for the processor under Article 28(3) and (4) GDPR.

78.   Moreover, the parties must commit themselves to mutual assistance and support. In addition to the obligation already set out in Clause 5 of Module Four, this also concerns the obligation of the processor to inform the controller of personal data breaches (Article 33(2) GDPR), which should be explicitly included in the agreement.

4.3.5   Horizontal remarks - Clause 2 (Local laws affecting compliance with the Clauses) and Clause 3 (Obligations of the data importer in case of government access requests)

4.3.5.1   Partial exemption of application to Module Four

79.   Concerning the fact that Clauses 2 and 3 will apply to Module Four "*only if the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU*", the EDPB and the EDPS stress that Article 3(1) GDPR does not state that personal data processed by the processor in the EU shall (also) be collected in the EU for the processor obligations to be applied to them. Therefore, the EDPB and the EDPS call on the Commission to clarify the reasons why this exemption has been inserted, and to further assess whether this exemption is justified.

80. Moreover, the EDPB and the EDPS call on the Commission to clarify the notion of "*combination*" of the personal data received from the third country controller with personal data collected by the processor in the EU, and the situations where this combination will take place, as such notion of combination of data is not envisaged in the GDPR.

4.3.5.2   Situations covered by Clauses 2 and 3

81. Concerning the situations covered in Clauses 2 and 3, the EDPB and the EDPS note that the scope of these provisions should be clarified. Indeed, it is not entirely clear if these clauses cover situations where, in the absence of legislation in the third country affecting compliance with the commitments of the data importer, practices affecting such compliance would still have to be taken into account and assessed, or even if the clauses will cover practices diverging from what the legal framework of the third country provides. For instance, concerning access to data by public authorities in the third country, even if not envisaged by the applicable legal framework, such access could take place in practice, or the authorities might access to the data without complying with the legal framework. In order to expressly take into account these situations, the titles of these clauses should be amended accordingly (in particular the title of Clause 2, which only refers to the laws, should be completed), and the wording of the clauses should be clarified to include more expressly these situations.

82. In particular, Clause 2(a) does not seem to impose any specific obligation in the case where there is no law relating to public authorities' access to personal data. In this respect, it is recalled that the EDPB Recommendations on supplementary measures provide that, in the absence of publicly available legislation, the data exporter should still look into other relevant and objective factors. The rationale behind this recommendation is that it cannot be reasonably inferred from the absence of law on public authorities' access to personal data that no access takes place in practice.

83. Therefore, the EDPB and the EDPS recommend to complement Clauses 2 and 3 to provide safeguards also in situations where the third country does not have a legislation, but where such practices, which would then be contrary to EU data protection requirements, exist or where the practice will diverge from the provisions of the legal framework. In particular, it should thus be clarified in the Draft SCCs that, in the absence of laws in the third country relating to public authorities' access to personal data, the parties should nevertheless, based on any available information, strive to identify any practice applicable to the data transferred preventing the data importer from fulfilling its obligations.

4.3.5.3   Scope of Clauses 2 And 3

84. Also concerning the scope of the clauses, the EDPB and the EDPS note that some elements such as the reference to the "*absence of requests for disclosure from public authorities received by the data importer*" or to "*relevant practical experience*" in this regard in Clause 2(b), as well as the use of the present tense in Clause 2(e) concerning the moment in which the data importer "*is or has become subject to laws not in line with the requirements under paragraph a)*" of Clause 2, are source of ambiguity. Indeed, these elements may give the impression that even when the prior assessment of the legal framework of the third country of the importer led to the conclusion that the legislation of the third country is not compliant with the EU requirements in terms of level of protection afforded to personal data and that no effective supplementary measure(s) could be put in place, transfers could still take place. The EDPB and the EDPS therefore recommend to clarify that these clauses will apply only to situations where, at the time of the conclusion of the contract, either the relevant law(s) of the third country was (were) assessed to be providing an essentially equivalent level of protection to that guaranteed within the EU, or where effective supplementary measures to remedy the potential deficiencies identified in such legislation and/or practices and to ensure the effective application of the safeguards contained in the Draft SCCs have been put in place so as to allow the data importer to comply with its obligations, or where the third country does not have any law in the field relevant to the transferred data.

85. In other words, the mechanisms foreseen in these clauses will be triggered only in cases where, either:

➢ The third country will have no legislation, but a practice incompliant with the EU requirements will be revealed;

➢ A change of law in the third country will occur, and as a consequence of this change, the legal framework of the third country of the importer will not be providing an essentially equivalent level of data protection anymore, which will thus require a suspension of the transfers taking place on the basis of the SCCs; or

➢ The implementation of the law will diverge in practice and no longer provide an essentially equivalent level of protection to that guaranteed within the EU.

4.3.6 Clause 2 – Local laws affecting compliance with the Clauses

4.3.6.1 Objective assessment of the legislation of the third country

86. The EDPB and the EDPS stress that the assessment of whether there is anything in the law or practice of the third country of destination, which prevents the data importer from fulfilling its obligations under the Draft SCCs in the context of the specific transfer, should be based on objective factors, regardless of the likelihood of access to the personal data. As underlined in the EDPB Recommendations on supplementary measures (in particular paragraphs 33 and 42[30], this assessment depends on the circumstances of the transfer and in particular on the following objective factors:

➢ Purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials);

➢ Types of entities involved in the processing (public/private; controller/processor);

➢ Sector in which the transfer occurs (e.g. adtech, telecommunication, financial, etc.);

➢ Categories of personal data transferred (e.g. personal data relating to children may fall within the scope of specific legislation in the third country);

➢ Whether the data will be stored in the third country or whether there is only remote access to data stored within the EU/EEA;

➢ Format of the data to be transferred (i.e. in plain text/ pseudonymised or encrypted);

➢ Possibility that the data may be subject to onward transfers from the third country to another third country.

87. In this respect, the EDPB and the EDPS also recall that in the Schrems II ruling, the CJEU did not refer to any subjective factor such as the likelihood of access, for instance. The mere fact that the data are comprised within the scope of a third country legislation that allows access to data by public authorities without specific essential guarantees (as recalled in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures[31]) would amount, *per se,* to considering that such access will possibly take place, without the need to rely on any practical

---

[30] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymea
suresransferstools_en.pdf.

[31] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguar
anteessurveillance_en.pdf.

experience in this regard or absence of requests for disclosure from public authorities received by the data importer. The current drafting of Clause 2(b)(i) can therefore be misunderstood as it might be read as permitting data to be exported if the data importer has not yet received any order to disclose personal data, even if it is subject to local laws permitting such orders. It could also be understood to allow continuing the transfer where the data importer is simply not permitted to inform the data exporter in this respect due to a gag order. Furthermore, assessing these kinds of subjective factors (likelihood of access) in practice would prove to be very difficult and hardly verifiable.

88.   Therefore, the EDPB and the EDPS recommend:

> ➢ Deleting the reference to "*the content and duration of the contract*"; "*the scale and regularity of transfers*"; "*the number of actors involved and the transmission channels used*"; "*any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer*";

> ➢ Ensuring full consistency between Clause 2(b)(i) and of the EDPB Recommendations on supplementary measures;

> ➢ Amending Clause 2(b)(ii) accordingly.

4.3.6.2   New annex to be added to the Draft SCCs

89.   In order to avoid that the parties merely agree to document the above-mentioned assessment without doing so in practice, the EDPB and the EDPS recommend to add an annex to the Draft SCCs to require the parties to document, prior to the signature of the contract, this assessment led under Clause 2 (i.e., the assessment of the third country's legislation and practices in the light of the circumstances of the transfer). This would help to achieve that the Draft SCCs will be correctly used, as an explicit annex would point the data importers and data exporters to the necessity of this assessment.

4.3.6.3   Consultation of the SA on supplementary measures

90.   Under Clause 2(f), the Draft SCCs provide for the consultation of the competent supervisory authority ("**SA**"). As underlined in the EDPB Recommendations on supplementary measures, "*when you intend to put in place supplementary measures in addition to SCCs, there is no need for you to request an authorisation from the competent SA to add these kind of clauses or additional safeguards as long as the identified supplementary measures do not contradict, directly or indirectly, the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined*."[32]

91.   Indeed, it is the responsibility of the data exporter, with the assistance of the data importer, to identify those measures. This is in line with the principle of accountability of Article 5(2) GDPR, which requires controllers to be responsible for, and be able to demonstrate compliance with the GDPR principles relating to processing of personal data. This was emphasized by the CJEU in its Schrems II ruling[33], and recalled in the EDPB Recommendations on supplementary measures[34].

---

[32] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymea surestransferstools_en.pdf; para 56

[33] Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems; Case C-311/18; para 134.

[34] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymea surestransferstools_en.pdf; para 5.

92. Also, the EDPB and the EDPS underline that there is no express legal basis in the GDPR according to which the SAs would have to provide for such kind of consultation.

4.3.6.4   Notification of SAs where the data exporters intend to continue with the transfers, even though no supplementary measures could be found

93. The EDPB and the EDPS recall that in previous SCCs, the data exporter had to "*forward*" the notification made by the data importer relating to the impossibility to respect the SCCs to the SA, where it "*decides, notwithstanding that notification, to continue the transfer or to lift the suspension*". This commitment, scrutinized by the CJEU in the Schrems II ruling, paragraph 145, should be retained in the Draft SCCs.

94. In line with the provisions contained in the 2010 SCCs[35], as scrutinized by the CJEU, a notification should be foreseen only if the data exporter intends to continue the transfer in the absence of effective supplementary measures. This case is not reflected in the Draft SCCs yet, while it is indeed the situation where a SA could have a role to play, and could intervene with its powers to suspend or prohibit data transfers in those cases where it finds that an essentially equivalent level of protection cannot be ensured in accordance with the Schrems II ruling[36].

95. In addition, the drafting of Clause 2(f) should make clear that such notification will not, in any way, constitute an authorisation to continue the transfer in the absence of suitable supplementary measures on the basis of the Draft SCCs. The EDPB and the EDPS thus call on the Commission to clarify this point.

4.3.7   Clause 3 – Obligations of the data importer in case of government access requests

96. The EDPB and the EDPS recommend clarifying that access requests from courts and other public authorities of the third country fall within the scope of this provision. This could for instance be achieved with a modification of the title of this clause.

4.3.7.1   Clause 3.1 – Notification

97. Under Clause 3.1, the EDPB and the EDPS underline that it should be clarified that the notification foreseen by the data importer would take place <u>before</u> having replied to the access request by third country's public authorities, so as to allow the data exporter to take any appropriate further steps, if needed.

4.3.7.2   Clause 3.2 – Review of legality and data minimisation

98. The EDPB and the EDPS understand that the scope of Clause 3.2 is limited to situations where access requests received by the data importer will not be compliant with the legislation of the third country, including its obligations resulting from international law and its rules governing conflicts of laws situations. The EDPB and the EDPS consequently recommend clarifying this clause in order to ensure that data exporters do not misunderstand it. This clause is only meant to ensure that the legislation of the third country already complying with EU law requirements will be applied correctly in that third

---

[35] 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council; OJ L 39, 12.2.2010, p. 5–18; Annex - Clause 4(g).
[36] Judgment of the Court (Grand Chamber) of 16 July 2020; Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems; Case C-311/18; para 113 and 121.

country. Therefore, this clause will not, *per se,* result in challenging the legality of requests of disclosure against EU data protection requirements, unless the legislation of the third country expressly provides for the possibility to invoke the legislation of another country.

4.3.8   Clause 5 - Data subject rights - Module One (Transfer controller to controller)

- **Clause 5(a)**

99.   According to this subparagraph, the data importer is responsible for dealing with data subjects' requests to exercise their rights. Possible difficulties may arise in practice, due to the data importer being outside the EU. For that reason, the EDPB and the EDPS share the view that this clause should be more closely aligned with the current requirements under the 2004 SCCs, i.e., the data exporter is in charge of responding to data subjects' enquiries, unless the parties agreed otherwise[37]. Besides, the parties should commit to assist and cooperate with each other when handling data subjects' requests.

100.   Additionally, the EDPB and the EDPS are of the opinion that the obligation imposed on the data importer to provide information to data subjects upon request should be clearly introduced in the Draft SCCs, and fully aligned with the requirements under Article 12(1) and Article 15 GDPR.

- **Clause 5(b)**

101.   In the opinion of the EDPB and the EDPS, data subjects should have the right to access, upon request, to more information than those currently listed under Clause 5(b)(i), and more precisely to:

➢   More precise information in relation to onward transfers, including for sub-processors, i.e., the full name and contact details of all recipients of the data relating to them[38]. This could be achieved by requiring the parties to provide such information in Annex III of the Draft SCCs, or by requiring to provide them to data subjects upon request;

➢   In accordance with Article 15(1)(d) GDPR, precise information on the envisaged period for which the personal data will be stored, where possible, or if not, the criteria used to determine that period. This could be achieved by requiring the parties to provide such information in Annex I of the Draft SCCs. Providing such information in Annex I might also make it clear to the parties that they need to actually define and implement retention periods; and

➢   In accordance with Article 15(1)(g) GDPR, any available information as to the source of collection, where the personal data are not collected directly from data subjects.

102.   Module One should include the data importer's obligation to inform data subjects on their rights to request rectification or erasure of their personal data, as well as their rights to request restriction of or to object to the processing of their personal data, which would bring this clause in line with Article 15(1)(e) GDPR. Such information would come in addition to information on the right to lodge a complaint with the competent SA, as currently included under Clause 5(b)(i). More generally, the EDPB and the EDPS call on the Commission to insert the obligation for the data importer to allow data subjects to exercise their right to request the restriction of the processing of their data.

---

[37] See clause 1(d) and Clause II(e) in 2004 SCCs.
[38] See Judgment of the Court (Third Chamber) of 7 May 2009; CJEU College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer C-553/07; para 49 and 54.

103.   As to Clause 5(b)(iii) concerning erasure of data subjects' personal data, the EDPB and the EDPS are of the opinion that such commitment should completely reflect the requirements set out in Article 17(1) GDPR.

- **Clause 5(c)**

104.   The EDPB and the EDPS are of the opinion that it is not justified to limit the right to object to direct marketing cases and that the scope of the right to object should be extended, especially in cases where the right to object is enforceable against the data exporter in the first place.

- **Clause 5(d)**

105.   The EDPB and the EDPS are of the opinion that the wording of Clause 5(d) should be revised so as to mirror Article 22 GDPR's prohibition of automated decision-making as a principle, and should set out the conditions allowing derogations to such prohibition. Clause 5(d) should also clarify that the data importer's obligations to implement suitable safeguards and provide information about the envisaged automated decision to data subjects are cumulative.

106.   In addition, in accordance with Article 22 and Article 15(1)(h) GDPR, Clause 5(d) should require that information provided to data subjects include the significance and the envisaged consequences for data subjects.

- **Clause 5(f)**

107.   Whilst the EDPB and the EDPS acknowledge that there may be circumstances justifying that the data importer may refuse a data subject's request, it should be made clear in the Draft SCCs that only the requirements of local 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 should be taken into account under this Clause.

- **Clause 5(g)**

108.   In order for data subjects to be fully able to exercise their rights, the EDPB and the EDPS consider that the obligation to inform data subjects that the data importer intends to reject their requests should be aligned with Article 12(4) GDPR, hence be provided without delay and at the latest within one month of receipt of the request.

4.3.9   Clause 5 - Data subject rights - Modules Two (Transfer controller to processor) and Three (Transfer processor to processor)

109.   Clause 5 in Module Two and Clause 5 in Module Three contain the same requirements, hence are addressed together in this Joint Opinion.

110.   The EDPB and the EDPS share the opinion that Clause 5(a) should:

- ➢ Further specify that the responses to data subjects shall be made in accordance with the controller's instructions (e.g. on content of the response) as set out in annex to the Draft SCCs.

- ➢ Further specify that the scope of the data importer's obligation relating to the exercise of data subjects' rights on behalf of the controller should be described and clearly set out in annex to the Draft SCCs.

4.3.10 Clause 5 - Data subject rights - Module Four (Transfer processor to controller)

111. The EDPB and the EDPS would welcome clarification from the European Commission regarding the possible practical consequences entailed by the commitment made by the parties to assist each other in handling data subjects' requests made on the basis of the data importer's applicable law.

112. The EDPB and the EDPS would welcome further clarity on the situations that the commitment made by the parties to assist each other in handling data subjects' aim at covering.

113. Moreover, it is unclear what is meant in Clause 5, where reference is made to the assistance "*for data processing by the data exporter in the EU, under the GDPR*". If the intention is, for instance, to cover assistance in relation to security obligations, it should be clarified by the Commission in the Draft SCCs.

4.3.11 Clause 6 - Redress

114. The EDPB and the EDPS would welcome clarification in the Draft SCCs as to whether the option to offer data subjects the possibility to seek redress before an independent dispute resolution body, at no cost, has to be provided in all sets of clauses. While it would be clear that this option may help ensure effective enforcement in case of controller to controller transfer, the EDPB and the EDPS would welcome further clarification as to how this mechanism will apply in Modules Two, Three, and Four. For instance, it should be clarified to which extent this mechanism would apply in relation to the specific and direct obligations of the processor and of the controller in Module Four.

115. As for the clauses on redress envisaged in Modules One, Two, and Three (Clause 6(b)), the EDPB and the EDPS are of the opinion that it should be made clearer that the data importer shall accept the right of the data subject (who invokes his or her rights as a third party beneficiary) to lodge directly a complaint with an EEA SA and/or bring a claim before an EEA court without the need to seek an amicable resolution of the dispute in advance. In fact, in order to ensure the same level of protection envisaged by Articles 77 and 79 GDPR, such type of mechanisms (e.g. internal complaint-handling mechanisms put in place by the data importer) should be encouraged so as to facilitate the exercise of the third party beneficiary rights, but they should not be considered as a prerequisite for lodging a complaint with the SA or with a court.

116. Furthermore, Article 77(1) GDPR provides that data subjects shall be able to choose to lodge a claim before the SA of their habitual residence, place of work, or place of the alleged infringement. From this perspective, the EDPB and the EDPS consider it to be important to amend Clause 6(b)(i) accordingly – as the Draft SCCs seem to refer only to the SA with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer.

117. The EDPB and the EDPS call for clarifications in relation to the absence of a redress clause in Module Four. Taking into consideration the commitments currently contained in Clause 5 of Module Four in relation to 'data processing by the data exporter in the EU, under the GDPR', the EDPB and the EDPS are wondering how the data subject's right to redress will be recognised in such cases.

4.3.12 Clause 7 - Liability - Modules One (Transfer controller to controller) and Four (Transfer processor to controller)

118. In Clause 7, Modules One and Four, the EDPB and the EDPS note that the joint and several liability towards the data subject would only be triggered in case there is a shared responsibility. In other words, the liability regime envisaged in the Draft SCCs does not provide for a full joint and several liability where each party would be responsible for the damage solely caused by the other party.

119. In this context, the EDPB and the EDPS would like to recall that the Draft SCCs should incorporate effective mechanisms that make it possible, in practice, to ensure compliance with the level of

protection required by EU law[39]. However, bringing an action against a non-EU company may prove to be difficult for the data subject as regards enforcement of the judgment against that non-EU company. The existing sets of SCCs are more protective than what is proposed in the Draft SCCs, and the EDPB and the EDPS are of the opinion that the protection of data subjects should be reinforced in this regard.

120. Against this background, the EDPB and the EDPS call for an amendment of Clause 7 in line with the considerations made above.

4.3.13 Clause 7 - Liability - Modules Two (Transfer controller to processor) and Three (Transfer processor to processor)

121. In Modules Two and Three, Clause 7(c) and 7(d), it is envisaged that the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer caused, against the data importer (c) or against the data exporter (d).

122. For the avoidance of doubt, it should be clarified in the Draft SCCs by the Commission that these possibilities are cumulative and the data subject has a choice to receive compensation, for any material or non-material damages the data importer caused, either against the data importer or the data exporter. In other words, the possibility to seek the liability of the data exporter for any material or non-material damages caused by the data importer should not be conditioned by an action against the data importer.

4.3.14 Clause 9 - Supervision

123. Clause 9 requires to specify the SA which is competent for the data exporter for the purpose of compliance with the Draft SCCs, but does not envisage the case where there may be several competent SAs if there are several data exporters as parties to the Draft SCCs (which is a possibility offered by the Draft SCCs). The EDPB and the EDPS would suggest clarifying this aspect by referring to the possibility that more than one EEA SA could be competent if different data exporters are involved and that, in this specific case, each SA with the responsibility to ensure compliance by the data exporter will be competent for the specific transfer carried out on its territory. For the sake of clarity and readability, the parties should be requested to designate the competent SAs in the annexes.

4.4   Section III - Final provisions

4.4.1   Clause 1 - Non-compliance with the Clauses and termination

124. Clause 1(d) provides for an exception to the obligation to return or destroy the data prior to the termination of the contract when the local law applicable to the data importer prohibits this return or destruction. The EDPB and the EDPS call the Commission to recall that the obligations of the data importer under Clause 5 Section II would also apply in the case referred to in Clause 1(d) Section III. The EDPB and the EDPS consider that the Commission should clarify in the Draft SCCs that only the requirements of local 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 should be taken into account under this clause.

---

[39] For instance, Article 47(2)(f) GDPR requires that BCRs shall specify, amongst others, "*the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union*".

125. In addition, the EDPB and the EDPS note that Clause 1(d) provides that the data importer should warrant that it will ensure, "*to the extent possible*" the level of protection required by these clauses.

126. In this respect, the EDPB and the EDPS recall that the level of protection required by the Draft SCCs should always be ensured. Therefore, the EDPB and the EDPS call on the Commission to remove the reference to "*to the extent possible*".

4.5 Annexes

127. The EDPB and the EDPS note that the Draft SCCs are designed to be possibly used – as a Multi Party Agreement - by more than one party as data exporters and/or as data importers. In order to avoid the risk of blurring roles and responsibilities, it is important to provide the parties, in the Draft SCCs, with clear indications as to how the Annex should to be filled out appropriately. This is all the more necessary because of the modular approach that allows the clauses to be incorporated within one Multi Party Agreement covering up to four scenarios (controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller transfers), and possibly a large number of transfers, each of them possibly occurring between different data exporters and/or data importers. The EDPB and the EDPS are therefore of the opinion that it is of utmost importance that the contract that will be signed in practice, including its Annexes, will, with absolute clarity, delimit the roles and responsibilities of each of the parties (data exporter-controller, data exporter-processor, data importer-controller, data importer-processor) in each relationship, and with regard to each transfer or set of transfers covered.

128. For these reasons, the Annex to the contract should be precise enough so it is possible at any point in time to determine who takes which role as regards a specific transfer or set of transfers of personal data. The EDPB and the EDPS therefore suggest to clarify that **each transfer or set of transfers**, i. e. each transfer or set of transfers carried out for one or several certain and defined purposes, should be separately described on the basis of its/their purpose(s), the types of personal data transferred, the category or categories of data subjects, the type(s) of processing, and the parties to the transfer (data importer(s) and data exporter(s)), as well as the role of the respective parties (controller(s) or processor(s)). Consequently, as a rule, a distinct Annex – which should include Parts I to VI - per transfer or set of transfers, will always be required. Such distinct Annex required for each transfer or set of transfers should be signed only by those data exporters and data importers which carry out the respective transfer. At the same time, each data exporter and data importer signing the respective Annex should specify, when signing the Annex relating to the respective transfer or the respective set of transfers, its role as regards this transfer or set of transfers (controller or processor), in order to avoid any ambiguities.

129. As a result, in case of a Multi Party Agreement addressing several transfers and/or parties, it should always be clear which Annex (comprising Parts I to VI) applies to which specific transfer or set of transfer, who the data exporters and data importers involved in that transfer or set of transfers are, and which role (controller or processor) the respective data exporter or data importer takes in that transfer or set of transfers. To this aim, the EDPB and the EDPS suggest to include some explanatory wording, in the "Annex" part of the Draft SCCs, aimed at guiding the parties on the appropriate use and signing of the Annex, in particular in the case of the Draft SCCs being used as a Multi Party Agreement. The EDPB and the EDPS have provided some corresponding wording suggestions in the technical annex of this Joint Opinion.

130. Thus, an Annex containing only general information that applies to a variety of transfers should not be considered complete. In order to avoid confusion, the Annex should be signed only by the parties that effectively carry out the specific processing, including those parties acceding to the clauses on the basis of Section I Clause 6.

131. Another problem encountered in practice, is that SCCs Annexes on technical and organisational measures are often filled out in a very generic way because they are meant to be made fit for a whole variety of different transfers and processing operations, while lacking precise indication as to which technical and organisational measures apply to which of the transfers covered by the SCCs. Therefore, the EDPB and the EDPS suggest to expressly highlight in the Draft SCC (Part III of the Annex as suggested by the EDPB and the EDPS) that only those specific technical and organisational measures that will be applied to the respective transfer/set of transfers should be enumerated, while technical and organisational measures that will only apply to other transfers / categories of transfers covered by the same Multi Party Agreement should only be filled out in those Annex that relates to those respective transfers for their part.

132. As regards controller-processor relationships, the EDPB and the EDPS note that, in practice, there is sometimes confusion about the requirements relating to sub-processors. The requirements set out in the Draft SCCs to enlist each and every sub-processor should be specifically recalled and reflected in Part V of the Annex. Moreover, the EDPB and the EDPS would suggest to indicate (as Part V of the Annex as suggested) the list of intended sub-processors (including, per each, their location, the processing operation(s), and type of safeguards they have implemented) in order to enable the controller to authorise the use of the intended sub-processors as required by Article 28(2) GDPR. It would be, moreover, also useful to insert the sentence that the controller has authorised the use of the sub-processors mentioned in that list.

For the European Data Protection Supervisor   For the European Data Protection Board

The European Data Protection Supervisor   The Chair

(Wojciech Wiewiorowski)   (Andrea Jelinek)

EUROPEAN
COMMISSION

Brussels, XXX
[…](2020) XXX draft

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

<u>**ANNEX**</u>

STANDARD CONTRACTUAL CLAUSES

<u>**SECTION I**</u>

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses (the Clauses) is to ensure compliance with the requirements 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 (General Data Protection Regulation)[1] [for the transfer of personal data to a third country].

(b)   Parties:

　　　(i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

　　　(ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via an intermediary entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer").

have agreed to these standard data protection clauses (hereinafter: "Clauses").

(c)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1), and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to add or update information in the Annexes. This does not prevent the Parties from including 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

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to the Regulation (EU) 2016/679 also ensures compliance with Article 29(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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision […].

Commented [A1]: The EDPB and the EDPS note that references are made both to GDPR and Regulation (EU) 2016/679 throughout the Clauses and call for consistency in this regard.

Commented [A2]: The EDPB and the EDPS note that the definition of data importer includes a reference to personal data received "indirectly via an intermediary entity".

For the sake of clarity, the EDPB and the EDPS recommend clarifying the concept or deleting the reference.

rights or freedoms of data subjects. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the Regulation (EU) 2016/679

(d) These Clauses apply with respect to the transfer of personal data as specified in Clause 5 of Section I [*Description of the Transfer(s)*].

(e) Annexes I, II and III form an integral part of these Clauses.

Clause 2

Third party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third party beneficiaries, against the data exporter and / or data importer, with the following exceptions:

(i) Section I;

(ii) Section II - Module One: Clause 1.5 (d) and Clause 1.9(b); Module Two: Clause 1.9(a), (c), (d) and (e); Module Three: Clause 1.1 and Clause 1.9(a), (c), (d) and (e); Module Four: Clause 1.1, Clause 1.2 and Clause 1.3;

(iii) Section II, Clause 3.1 (c), (d) and (e);

(iv) Section II, Clause 4;

(v) Section II - Module One: Clause 7(a), (b); Modules Two and Three: Clause 7(a), (b);

(vi) Section II, Clause 8;

(vii) Section II, Clause 9;

(viii) Section III, Clause 1 and Clause 3(a), (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 3

Interpretation

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

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

(e) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

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 these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purposes for which they are transferred, are specified in Annex I.B [*Description of the transfer(s)*].

Clause 6 - Optional

Docking clause

(a) An entity that is not a Party to the Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer by completing Annex I.A [*List of Parties*], Annex I.B [*Description of the transfer(s)*], and Annex II [*Technical and organisational measures*] and Annex VI [Documentation of the main aspects of the assessment performed under Clause 2 (b) of Section II].

(b) Once Annex I.A. is completed and signed , the acceding entity shall be treated as a Party to these Clauses and shall have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding Party shall have no rights or obligations arising under these Clauses from the period prior to the date of signing Annex I.A.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 1

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

1.1 Purpose limitation

The data importer shall not process the personal data for any purposes that are incompatible with other than the specific, explicit and legitimate purpose(s) of the transfer, as set out in Annex I.B. [*Description of the transfer(s)*], unless it has obtained the data subject's prior consent.

1.2 Transparency

(a)   In order to enable data subjects to effectively exercise their rights pursuant to Clause 5 of Section II, the data importer shall inform them, either directly or through the data exporter:

    (i)   of its identity and contact details;

    (ii)   where, in accordance with Clause 1.1 of Section II, it intends to process the personal data received from the data exporter for a different purpose than the purpose(s) of the transfer pursuant to Annex I.B. [*Description of the transfer(s)*], of that different purpose;

    (ii)(iii)   the categories of personal data processed,

    (iii)(iv)   the period for which the personal data will be stored, or if that is not possible the criteria used to determine the period

    (iv)(v)   where it intends to disclose the personal data to any third party, in accordance with Clause 1.7 of Section II, of the identity of that third party and the purpose of such disclosure.

> **Commented [A10]:** For the sake of clarity, the EDPB and the EDPS recommend referring to Clause 1.1 of Section II.

> **Commented [A11]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.1.2 of the Joint Opinion.

> **Commented [A12]:** For the sake of clarity, the EDPB and the EDPS recommend referring to Clause 1.7 of Section II.

(b)   Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing such information proves impossible or would involve a disproportionate effort. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c)   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, the Parties may redact part of 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.

> **Commented [A13]:** The EDPB and the EDPS consider that it is rather unlikely that business secrets would justify redacting entirely the annexes, which may contain useful elements for the data subject who has a right to obtain information about the processing, which includes information on recipients (processors and sub processors) and the safeguards implemented.
>
> Therefore, the EDPB and the EDPS recommend to specify that only part of the annexes may be redacted.

(d)   Subparagraphs (a) to (c) are 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.

1.3   Accuracy and data minimisation

(a)   The Parties shall ensure that the personal data is accurate and kept up to date, to the extent necessary having regard to the purpose(s) of processing. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b)   If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c)   The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

1.4   Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all of its back-ups at the end of the retention period.

1.5 Security of processing

(a) The data importer and, ~~during the transmission, also~~ the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter " personal data breach") including during the transmission by the data exporter to the data importer. In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the risks involved in the processing for the data subjects and their severity, the nature of the personal data and the nature, scope, context and purposes of processing, and in particular consider encryption during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling the purpose of processing. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer 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 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.

(c) In the event of a data breach concerning personal data processed by the data importer, the data importer shall take appropriate measures to address the data breach, including measures to mitigate its possible adverse effects.

(d) ~~If a data breach is likely to result in significant adverse effects,~~ Unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay, and where feasible, not later than 72 hours after having become aware of it, —notify both the data exporter and the competent supervisory authority within the meaning of Clause 9 of Section II [*Supervision*]. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the data breach and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide the information at the same time, it may do so in phases without undue further delay.

(e) In addition, if a data breach is likely to result in a high risk to the rights and freedoms of natural persons, in such cases, the data importer shall also, if necessary in cooperation with the data exporter, notify without undue delay the data subjects concerned of the data breach, together with a description in clear and plain language of the nature of the personal data breach and the information referred to in

---

[2] In line with recital 26 of the Regulation (EU) 2016/679, this requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, and that this process is irreversible.

Commented [A14]: For the sake of clarity, the EDPB and the EDPS recommend to move "during the transmission" at the end of the sentence to make it clearer that both parties have an obligation in line with Article 32 GDPR to ensure security of personal data, not only in relation to transmission but also for data at rest.

Commented [A15]: The EDPB and the EDPS recommend to make a reference to an annex describing precisely the said measures.

Commented [A16]: The EDPB and the EDPS recommend aligning the definition of personal data breach with the one set out by Article 4(12) GDPR.

Commented [A17]: For the sake of clarity, the EDPB and the EDPS recommend to clarify the role of each party with respect to transmission, as it may not be entirely clear from the initial wording.

Commented [A18]: For the sake of clarity, the EDPB and the EDPS recommend referring to the wording of Article 32 GDPR.

Commented [A19]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.1.3 of the Joint Opinion.

Commented [A20]: The EDPB and the EDPS note that this provision applies to Module 2 and 3 and consider it is also appropriate for Module 1.

Commented [A21]: The EDPB and the EDPS recommend to clarify who the authorized persons are and whether the concept notably includes the "intermediary" referred in Clause 1(b) of Section I.

Commented [A22]: The EDPB and the EDPS recommend aligning the wording with Article 33(1) GDPR.

Commented [A23]: The EDPB and the EDPS recommend aligning the wording with Article 34(1) GDPR.

Commented [A24]: The EDPB and the EDPS recommend aligning the wording with Article 34(2) GDPR.

subparagraph (de), ii) to iv), unless this would involve disproportionate efforts. In the latter case, the data importer shall instead make a public communication or similar measure whereby data subjects are informed in an equally effective manner.

(f) The data importer shall document all relevant facts relating to the data breach, including its effects and any remedial action taken, and keep a record thereof.

1.6 Special categories of personal data

To the extent the transfer includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, 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 security measures (such as pseudonymisation) or additional restrictions with respect to further disclosure.

1.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses and is able to comply with all stipulations of these Clauses. Alternatively, an onward transfer by the data importer may only take place if:

(i) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation (EU) 2016/679 with respect to the processing in question and is able to comply with all stipulations contained in those safeguards;

(ii) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 Regulation (EU) 2016/679 that covers the onward transfer;

(iii) the third party enters into an agreement with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter; or

(iv) the data importer has obtained the explicit consent of the data subject, after having informed him / her of the purpose(s) of the onward transfer, the identity and contact details of recipient(s) or categories of recipients, the countries to which personal data is transferred and the fact that whether they do not provide an adequate level of protection, and of the possible risks of such transfer to the data subject due to the lack of appropriate data protection safeguards for the onward transfer. In this case, the data importer shall inform the data exporter of

---

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

Commented [A25]: The EDPB and the EDPS understand that the reference should be made to subparagraph (d) and not (e).

Commented [A26]: The EDPB and the EDPS recommend to add this commitment in compliance with Article 34(3)(c) GDPR.

Commented [A27]: The EDPB and the EDPS recommend to refer separately to genetic data, in accordance with Article 9(1) GDPR.

Commented [A28]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

Commented [A29]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

Commented [A30]: In accordance with the GDPR, the order to be considered is first adequacy and then appropriate safeguards.

Therefore, the EDPB and the EDPS recommend to refer to (ii) before (i).

Commented [A31]: The EDPS and the EDPB recommend the suggested amendment in order to ensure consistency with Clause 1(2)(a) on Transparency which provides for an obligation to inform data subjects with the identity of the third party to which the data are disclosed.

Commented [A32]: The EDPB and the EDPS recommend this amendment in line with the EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en)

the onward transfer and, at the request of the data exporter, shall provide a copy of the information provided to the data subject.

> **Commented [A33]:** For the sake of clarity, the EDPB and the EDPS recommend this amendment.

Any ~~disclosure~~ onward transfer may only take place subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

> **Commented [A34]:** The term "disclosure" may be confusing as often used in the context of government data access.
>
> Therefore, the EDPB and the EDPS recommend to replace this term by "onward transfer" which is the subject of this clause.

1.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, does not process the data except on instructions from the data importer.

1.9 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities under its responsibility.

(b) The data importer and the data exporter shall make such documentation available to the competent supervisory authority on request.

> **Commented [A35]:** The EDPB and the EDPS consider that the data exporter should also be subject to this obligation.

MODULE TWO: Transfer controller to processor

1.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give further instructions regarding the data processing, within the framework the contract agreed with the data importer, throughout the duration of the contract, but such instructions shall always be documented.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

> **Commented [A36]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.3.1 (para. 68) of the Joint Opinion, that also applies to Module 2.

1.2 Purpose limitation

The data importer shall process the personal data only for the specific, explicit and legitimate, purpose(s) of the transfer, specified by the data exporter, as set out in Annex I.B [*Description of the transfer(s)*].

> **Commented [A37]:** For the sake of clarity, the EDPB and the EDPS recommend aligning the wording with Article 5(1)(b) GDPR.

> **Commented [A38]:** For the avoidance of doubt, the EDPB and the EDPS recommend specifying that the purposes of the processing are set by the data exporter.

1.3 Transparency

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 part of 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.

> **Commented [A39]:** The EDPB and the EDPS consider that it is rather unlikely that business secrets would justify redacting entirely the annexes which may contain useful elements for the data subject who has a right to obtain information about the processing which includes information on recipients (processors and sub processors) and the safeguards implemented.
>
> Therefore, the EDPB and the EDPS recommend to specify that only part of the annexes may be redacted.

1.4   Accuracy

If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay. In this case the data importer shall cooperate with the data exporter to erase or rectify the data.

1.5   Storage limitation and erasure or return of data

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~~demonstrate 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 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.

1.6   Security of processing

(a)   The data importer and, ~~during the transmission, also~~ the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"), including during the transmission by the data exporter to the data importer. In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the risks involved in the processing for the data subjects and their severity, the nature of the personal data and the nature, scope, context and purposes of processing, and in particular consider encryption during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling the purpose of processing. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall where possible remain under the exclusive control of the data exporter. In complying with this obligation, the data importer shall implement at least the technical and organisational measures specified in Annex II [*Technical and organisational measures*]. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The data importer 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 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.

(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 the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information

---

Commented [A40]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.1 of the Joint Opinion.

Commented [A41]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment.

Commented [A42]: For the avoidance of doubt, the EDPB and the EDPS recommend replacing "notwithstanding" by "without prejudice to".

Commented [A43]: For the sake of clarity, the EDPB and the EDPS recommend to move "during the transmission" at the end of the sentence to make it clearer that both parties have an obligation in line with Article 32 GDPR to ensure security of personal data, not only in relation to transmission but also for data at rest.

Commented [A44]: The EDPB and the EDPS recommend aligning the definition of personal data breach on the one set out by Article 4(12) GDPR.

Commented [A45]: For the sake of clarity, the EDPB and the EDPS recommend to clarify the role of each party with respect to transmission, as it may not be entirely clear from the initial wording.

Commented [A46]: For the sake of clarity, the EDPB and the EDPS recommend referring to the wording of Article 32 GDPR.

Commented [A47]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.2 (para 60) of the Joint Opinion.

Commented [A48]: The EDPB and the EDPS consider that Annex II may only serve as a list of defined minimum requirements but should not serve as a definition of the required level of security.

Commented [A49]: The EDPS and the EDPB note that this obligation is provided for the data importer under Section II, Clause 1.5 (Module 1) and consider that it may also be appropriate in the context of Module 2.

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 be taken to mitigate its possible adverse effects. 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.

(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 the Regulation (EU) 2016/679, notably to 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.

> **Commented [A50]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.2 of the Joint Opinion.

1.7   Special categories of personal data

To the extent the transfer includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, 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 (hereinafter "special categories of data"), the data importer shall apply the specific restrictions and/or additional safeguards specified by the data exporter, as described in Annex I.B [*Description of the transfer(s)*].

> **Commented [A51]:** The EDPB and the EDPS recommend to refer separately to genetic data, in accordance with Article 9(1) GDPR.

> **Commented [A52]:** For the avoidance of doubt, the EDPB and the EDPS recommend specifying that the restrictions and/or safeguards are set by the data exporter.

1.8   Onward transfers

The data importer shall only disclose the personal data to a third party on the basis of documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses and is able to comply with all stipulations of these Clauses or, alternatively, an onward transfer by the data importer may only take place if:

(i)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation (EU) 2016/679 with respect to the processing in question and is able to comply with all stipulations contained in those safeguards;

(ii)   the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 Regulation (EU) 2016/679 that covers the onward transfer.

Any ~~disclosure~~ onward transfer may only take place subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

> **Commented [A53]:** For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

> **Commented [A54]:** For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country, which normally would require supplementary measures, would be permitted without supplementary measures.

> **Commented [A55]:** In accordance with the GDPR, the order to be considered is first adequacy and then appropriate safeguards.
>
> Therefore, the EDPB and the EDPS recommend to refer to (ii) before (i).

> **Commented [A56]:** The term "disclosure" may be confusing as often used in the context of government data access.
>
> Therefore, the EDPB and the EDPS recommend to replace this term by "onward transfer" which is the subject of this clause.

---

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

1.9 Documentation and compliance

(a) The data importer shall promptly and properly deal with inquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities performed on behalf of the data exporter and under its responsibility.

> **Commented [A57]:** For the sake of clarity, the EDPB and the EDPS recommend to clarify this provision as suggested.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and allow for and contribute to reviews of data files, systems, and documentation, ~~or~~ and allow for and contribute to ~~of~~ 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 data exporter may take into account relevant certifications held by the data importer.

> **Commented [A58]:** For the sake of clarity, the EDPB and the EDPS recommend to clarify the scope of the audit as suggested.

> **Commented [A59]:** The wording of the clause might suggest that only a review of audits (e.g. documentation) would be allowed.
>
> Therefore, the EDPB and the EDPS recommend to better reflect the provisions of Article 28(3)(h) GDPR.

(d) The data exporter may choose to conduct the audit by itself, or to mandate, at its own cost, an independent auditor ~~or to rely on an independent audit mandated by the data importer~~. ~~Where the data importer mandates an audit, it has to bear the costs of the independent auditor.~~ Audits may also include inspections at the premises or physical facilities of the data importer ~~and shall be carried out with reasonable notice~~.

> **Commented [A60]:** The wording of the clause might suggest that only a review of audits (e.g. documentation) would be allowed.
>
> Therefore, the EDPB and the EDPS recommend to better reflect the provisions of Article 28(3)(h) GDPR.

> **Commented [A61]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.4 of the Joint Opinion.

> **Commented [A62]:** The EDPB and the EDPS consider that 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.

(e) The data importer and the data exporter 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.

> **Commented [A63]:** 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 [A64]:** The EDPB and the EDPS consider that the data exporter should also be subject to this obligation.

> **Commented [A65]:** The EDPB and the EDPS recommend referring to the other annexes as well.

MODULE THREE: Transfer processor to processor

1.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of the controller(s) as specified in Annex I.A. [*List of parties*], which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further instructions regarding the data processing within the framework of the contract agreed with the data importer throughout the duration of the contract, but such instructions shall always be documented.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. To the extent the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller thereof.

> **Commented [A66]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.3.1 (para. 68) of the Joint Opinion.

1.2 Purpose limitation

The data importer shall process the personal data only for the specific, explicit, and legitimate purpose(s) of the transfer, specified by the controller, as set out in Annex I.B. [*Description of the transfer(s)*].

> **Commented [A67]:** For the sake of clarity, the EDPB and the EDPS recommend aligning the wording with Article 5(1)(b) GDPR.

> **Commented [A68]:** For the avoidance of doubt, the EDPB and the EDPS recommend specifying that the purposes of the processing are set by the controller.

1.3 Transparency

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, the Parties may redact part of 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.

1.4 Accuracy

If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party and the controller without undue delay. In this case the data importer shall cooperate with the data exporter and the controller to rectify or erase the data.

1.5 Storage limitation and erasure or return of data

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 controller and ~~certify~~demonstrate 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 guarantee, to the extent possible, the level of protection required by these Clauses and will only process ~~it~~ the personal data to the extent and for as long as required under that local law.

1.6 Security of processing

(a) The data importer and, ~~during the transmission, also~~ the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"), including during the transmission by the data exporter to the data importer. In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation the risks involved in the processing for the data subjects and their severity, the nature of the personal data and the nature, scope, context and purposes of processing, and in particular consider encryption during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling the purpose of processing. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall where possible remain under the exclusive control of the data exporter. In complying with this obligation, the data importer shall implement at least the technical and organisational measures specified in Annex II [*Technical and organisational measures*]. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

Commented [A69]: The EDPB and the EDPS consider that it is rather unlikely that business secrets would justify redacting entirely the annexes which may contain useful elements for the data subject who has a right to obtain information about the processing which includes information on recipients (processors and sub processors) and the safeguards implemented.

Therefore, the EDPB and the EDPS recommend to specify that only part of the annexes may be redacted.

Commented [A70]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.3.2 of the Joint Opinion.

Commented [A71]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment.

Commented [A72]: For the avoidance of doubt, the EDPB and the EDPS recommend replacing "notwithstanding" by "without prejudice to".

Commented [A73]: For the sake of clarity, the EDPB and the EDPS recommend this technical amendment.

Commented [A74]: For the sake of clarity, the EDPB and the EDPS recommend to move "during the transmission" at the end of the sentence to make it clearer that both parties have an obligation in line with Article 32 GDPR to ensure security of personal data, not only in relation to transmission but also for data at rest.

Commented [A75]: The EDPB and the EDPS recommend aligning the definition of personal data breach with those set out by Article 4(12) GDPR.

Commented [A76]: For the sake of clarity, the EDPB and the EDPS recommend to clarify the role of each party with respect to transmission, as it may not be entirely clear from the initial wording.

Commented [A77]: For the sake of clarity, the EDPB and the EDPS recommend referring to the wording of Article 32 GDPR.

Commented [A78]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.2 (para 61) of the Joint Opinion, which also applies to Module 3.

Commented [A79]: The EDPB and the EDPS consider that Annex II may only serve as a list of defined minimum requirements but should not serve as a definition of the required level of security.

Commented [A80]: The EDPS and the EDPB note that this obligation is provided for Module 1 and consider it is also appropriate for Module 3.

(b)   The data importer 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 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.

(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.

(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 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.

> **Commented [A81]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.3.3 of the Joint Opinion.

1.7   Special categories of personal data

To the extent the transfer includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, 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 (hereinafter "special categories of data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B [*Description of the transfer(s)*].

> **Commented [A82]:** The EDPB and the EDPS recommend to refer separately to genetic data, in accordance with Article 9(1) GDPR.

1.8   Onward transfers

The data importer shall only disclose the personal data to a third party on the basis of documented instructions from the controller. In addition, the data may only be disclosed to a third party located outside the European Union[5] (hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses and is able to comply with all stipulations of these Clauses or, alternatively, an onward transfer by the data importer may only take place if:

> **Commented [A83]:** For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

---

[5] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(i)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 GDPR and is able to comply with all stipulations of these Clauses;

(ii) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 GDPR that covers the onward transfer.

Any ~~disclosure~~ onward transfer may only take place subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

1.9   Documentation and compliance

(a)   The data importer shall promptly and properly deal with inquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b)   The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities performed on behalf of the controller and under its responsibility.

(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, systems and documentation, ~~or~~ and allow for and contribute to ~~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.

(d)   The controller or data exporter may choose to conduct the audit by itself or, to mandate, at its own cost, an independent auditor ~~or to rely on an independent audit mandated by the data importer. Where the data importer mandates an audit, it has to bear the costs of the independent auditor~~. Audits may also include inspections at the premises or physical facilities of the data importer ~~and shall be carried out with reasonable notice.~~.

(e)   The data importer and the data exporter 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.

MODULE FOUR: Transfer processor to controller

1.1   Instructions

(a)   The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b)   The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe the GDPR or other Union or Member State data protection law.

(c)   The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under the GDPR, including as regards cooperation with competent supervisory authorities.

Commented [A84]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

Commented [A85]: In accordance with the GDPR, the order to be considered is first adequacy and then appropriate safeguards.

Therefore, the EDPB and the EDPS recommend to refer to (ii) before (i).

Commented [A86]: The term "disclosure" may be confusing as often used in the context of government data access.

Therefore, the EDPB and the EDPS recommend to replace this term by "onward transfer" which is the subject of this clause.

Commented [A87]: For the sake of clarity, the EDPB and the EDPS recommend to clarify this provision as suggested.

Commented [A88]: The wording of the clause might suggest that only a review of audits (e.g. documentation) would be allowed.

Therefore, the EDPB and the EDPS recommend to better reflect the provisions of Article 28(3)(h) GDPR.

Commented [A89]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.4 of the Joint Opinion, which also applies to Module 3.

Commented [A90]: The EDPB and the EDPS consider that 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 [A91]: 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 [A92]: The EDPB and the EDPS consider that the data exporter should also be subject to this obligation.

1.2 Security of processing

The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during the transmission to the data importer, 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 state of the art the costs of implementation, the risks involved in the processing for the data subjects and their severity, the nature of the personal data[6] and the nature, scope, context and purposes of processing, and in particular consider encryption during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling the purpose of processing. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security

1.3 Documentation and compliance

(a)   The Parties shall be able to demonstrate compliance with these Clauses. The Parties data importer shall make available to each other the data exporter and the controller all information necessary to demonstrate compliance with its obligations set out in these Clauses.

(b)   The data exporter and the data importer shall make the information referred to in paragraph (a) available to the competent supervisory authority on request-.

> **Commented [A93]:** For the sake of clarity, the EDPB and the EDPS recommend referring to the wording of Article 32 GDPR.

> **Commented [A94]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.2 (para 61) of the Joint Opinion, which also applies to Module 4.

> **Commented [A95]:** The EDPS and the EDPB note that this obligation is provided for Module 1 and consider it is also appropriate for Module 4.

> **Commented [A96]:** The EDPB and the EDPS recommend inserting these additional provisions mirroring what is provided for in Module 2 and 3.

Clause 2

Local laws affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(only if the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a)   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 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

---

[6] This includes whether the transfer and further 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 or offences.

proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses.

(b)   The Parties declare that in providing the warranty in paragraph a, they have taken due account in particular of the following elements:

> **Commented [A97]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comments made in Section 4.3.6.1 of the Joint Opinion.

(i)   the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred;

(ii)   the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards;

(iii)   any safeguards in addition to those under these Clauses, including the contractual, technical and organisational measures applied by the data exporter during transmission to the data importer and to the processing ~~of the personal data in the country of destination~~ by the data importer.

> **Commented [A98]:** The EDPB and the EDPS recommend to clarify as suggested.

(c)   The data importer warrants that, in carrying out the assessment under paragraph b), it has made best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

> **Commented [A99]:** For Module 3, the EDPB and the EDPS consider that the controller as well should be considered.

(d)   The Parties have documented in Annex VI the main aspects of the assessment under paragraph b) and agree to. ~~The parties agree to document the assessment under paragraph b) and~~ make it available to the competent supervisory authority upon request.

> **Commented [A100]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.6.2 of the Joint Opinion.

(e)   The data importer agrees to promptly notify the data exporter if, after having agreed to these Clauses and for the duration of the contract , it has reason to believe that it is or has become subject to laws not in line with the requirements under paragraph a), including following a change of the laws in the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements under paragraph a).

> **Commented [A101]:** For Module 3, the EDPB and the EDPS consider that the controller as well should be notified.

(f)   Following a notification pursuant to paragraph e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under the Clauses, the data exporter shall promptly identify appropriate measures (such as, for instance, contractual, technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and / or data importer to address the

> **Commented [A102]:** For Module 3, the EDPB and the EDPS consider that the controller as well should be considered.

> **Commented [A103]:** For Module 3, the EDPB and the EDPS consider that the controller as well should be considered.

> **Commented [A104]:** The EDPB and the EDPS recommend to clarify as suggested.

situation, if appropriate in consultation with the [for Module Three: controller and] competent supervisory authority. If the data exporter decides to continue the transfer, based on its assessment that these additional measures will allow the data importer to fulfil its obligations under the Clauses, the data exporter shall forward the notification to the competent supervisory authority together with an explanation, including a description of the measures taken. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall inform the competent supervisory authority and shall be entitled to terminate the contract. In case 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. When the contract is terminated pursuant to this Clause, Section III, Clause 1 (d) and (e) shall apply.

> **Commented [A105]:** The EDPB and the EDPS recommend to clarify this notion of "responsible Party".

Clause 3

Obligations of the data importer in case of government access requests

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(only if the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

3.1 Notification

(a) 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:

> **Commented [A106]:** For Module 3, the EDPB and the EDPS consider that the controller as well should be notified.

   (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;

   (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 all information available to the importer.

   [For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and / or the data subject, the data importer agrees to use its best efforts to obtain a waiver of the

> **Commented [A107]:** For Module 3, the EDPB and the EDPS consider that the controller as well should be mentioned.

prohibition, with a view to communicate as much information and as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them upon request of the data exporter.

(c) To the extent permissible under the laws of the country of destination, the data importer agrees to provide to the data exporter, in regular intervals for the duration of the contract, the greatest possible amount of relevant information on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the data importer is or becomes partially or completely prohibited from providing the data exporter with the aforementioned information, it shall without undue delay inform the data exporter accordingly. [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs a) to c) for the duration of the contract and make it available to the competent supervisory authority upon request.

(e) Paragraphs a) to c) are notwithstanding the obligation of the data importer pursuant to Clause 2(e) of this Section and Clause 1 of Section III [*Termination*] to promptly inform the data exporter where it is unable to comply with these Clauses.

3.2 Review of legality and data minimisation

(a) 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.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Clause 4

Use of sub-processors

Commented [A108]: For the avoidance of doubt, the EDPB and the EDPS would like to propose the suggested amendment.

Commented [A109]: For the avoidance of doubt, the EDPB and the EDPS recommend replacing "notwithstanding" by "without prejudice to".

Commented [A110]: For the sake of completeness, the EDPB and the EDPS recommend the suggested amendment.

Commented [A111]: For Module 3, the EDPB and the EDPS consider that the controller as well should be informed.

Commented [A112]: For Module 3, the EDPB and the EDPS consider that this information should also be made available to the controller.

MODULE TWO: Transfer controller to processor

(a) OPTION 1 SPECIFIC PRIOR AUTHORISATION: The data importer shall not sub-contract 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. 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 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 specifically 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). 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 III up to date.

(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, including in terms of third party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Section II, Clause 1.8 [*Onward transfers*], provided that the sub-processor is able to comply with all stipulations of these Clauses- The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and subsequent amendments to the data exporter.

(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.

(e) The data importer shall agree a third party beneficiary clause with the sub-processor whereby, for instance in the event of bankruptcy of the data importer, the data exporter 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.

Commented [A113]: The EDPB and the EDPS would recommend to include this new sentence to reflect the following remark from the EDPB Guidelines 07/2020 on the concepts of controller and processor, 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 [A114]: The possibility to subscribe to a newsletter or similar measures should not satisfy the requirement.

Therefore, for the avoidance of doubt the EDPB and the EDPS recommend to clarify this provision as suggested.

Commented [A115]: The EDPB and the EDPS 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 [A116]: The EDPB and the EDPS 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.

Commented [A117]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

Commented [A118]: The EDPB and the EDPS consider that the controller must always have the possibility to instruct any sub-processor.

Therefore, the EDPB and the EDPS recommend not to restrict the third party beneficiary clause to the sole case of bankruptcy. Please see the suggested amendment.

MODULE THREE: Transfer processor to processor

(a)   OPTION 1 SPECIFIC PRIOR AUTHORISATION: The data importer shall not sub-contract any of its processing activities performed on behalf of the controller data exporter under these Clauses to a sub-processor without prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the concerned sub-processor. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller 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 controller'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 specifically inform the controller 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 controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). It shall inform the data exporter of such engagement. The Parties shall keep Annex III up to date.

(b)   Where the data importer engages a sub-processor for carrying out specific processing activities (on behalf of the controller), 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, including in terms of third party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Section II, Clause 1.8 [*Onward transfers*], provided that the sub-processor is able to comply with all stipulations of these Clauses. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)   The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and subsequent amendments.

(d)   The data importer shall remain fully responsible to the data exporter and the controller for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter who shall in turn notify the controller of any failure by the sub-processor to fulfil its obligations under that contract.

(e)   The data importer shall agree a third party beneficiary clause with the sub-processor whereby, for instance in the event of bankruptcy of the data importer, the data exporter and the controller shall each 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.

Clause 5

Data subject rights

Commented [A119]: The EDPB and the EDPS consider that the processing by processors and sub-processors is performed on behalf of the controller.

Commented [A120]: The possibility to subscribe to a newsletter or similar measures should not satisfy the requirement.

Therefore, for the avoidance of doubt the EDPB and the EDPS recommend to clarify this provision as suggested.

Commented [A121]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment. Otherwise, an onward transfer to a third country which normally would require supplementary measures would be permitted without supplementary measures.

Commented [A122]: The EDPB and the EDPS consider that the data importer should also remain fully responsible to the controller as the controller is required to ensure appropriate protection when data is transferred.

Commented [A123]: For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment.

Commented [A124]: The EDPB and the EDPS consider that the controller must always have the possibility to instruct any sub-processor.

Therefore, the EDPB and the EDPS recommend not to restrict the third party beneficiary clause to the sole case of bankruptcy. Please see the suggested amendment.

Commented [A125]: The EDPB and the EDPS recommend the suggested amendment since the controller is in the end the entity responsible for the processing operation.

MODULE ONE: Transfer controller to controller

(a) The data importer shall deal with any inquiries and requests it receives from a data subject relating to the processing of his / her personal data and the exercise of his / her rights under these Clauses without undue delay. The data importer shall take appropriate measures to facilitate such inquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge, without undue delay and at the latest within one month[7] of the receipt of the request:

   (i) provide confirmation to the data subject as to whether personal data concerning him / her is being processed and, where this is the case, provide a copy of the data relating to him / her as well as the information contained in Annex I (including, where the personal data are not collected from the data subject, any available information as to their source), information on onward transfers and information on the right to lodge a complaint with the competent supervisory authority;

   (ii) rectify inaccurate or incomplete data concerning the data subject;

   (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third party beneficiary rights.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) Where the data importer intends to make decisions based solely on the automated processing of the personal data transferred without human involvement (hereinafter "automated decisions"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, it shall, when necessary in cooperation with the data exporter:

   (i) inform the data subject about the envisaged automated decision and the logic involved;

   (ii) implement suitable safeguards, at least by enabling the data subject to contest the automated decision, express his / her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

| **Commented [A126]:** The EDPB and the EDPS recommend to also refer to this information, which does not seem to be encompassed by Annex I. |

---

[7] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(f)   The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) GDPR.

(g)   If the data importer intends to refuse a data subject's request, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the refusal and about the possibility of lodging a complaint with the competent supervisory authority and / or seeking judicial review.

> **Commented [A127]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.8 (para 108) of the Joint Opinion.

MODULE TWO: Transfer controller to processor

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

(b)   Taking into account the nature of the processing, the data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' inquiries and requests for the exercise of their rights under the GDPR.

MODULE THREE: Transfer processor to processor

(a)   The data importer shall promptly notify the data exporter and, where appropriate, the controller about any inquiry or request received directly from a data subject, without responding to that inquiry or request unless and until it has been otherwise authorised to do so by the controller.

(b)   Taking into account the nature of the processing, the data importer shall assist the controller in fulfilling its obligations to respond to data subjects' inquiries and requests for the exercise of their rights under the GDPR.

> **Commented [A128]:** The EDPB and the EDPS recommend aligning the wording with Module 2 above.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to inquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under the GDPR.

Clause 6

Redress

(a)   The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints or requests. It shall promptly deal with any complaints or requests by a data subject.

> **Commented [A129]:** The EDPB and the EDPS recommend that, where this information is already available to the data exporter, it should also be provided by it.

[OPTION: The data importer agrees that the data subject may also lodge a complaint with [*Insert name of an independent dispute resolution body*][8] at no cost to the data subject. It shall inform the data subject, in the manner set out in paragraph a), of this additional redress mechanism and that (s)he is not required to make use of such additional redress mechanism, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties agree that if there is a dispute between a data subject and one of the Parties as regards compliance with these Clauses, they shall keep each other informed about such proceedings and, where appropriate, cooperate in resolving the issue in a timely fashion.

(b) Where the dispute is not amicably resolved and the data subject invokes a third-party beneficiary right pursuant to Clause 2 of Section I, the data importer accepts the decision of the data subject to:

    (i) lodge a complaint with the competent supervisory authority within the meaning of Clause 9 of Section II [*Supervision*];

    (ii) refer the dispute to the competent courts within the meaning of Clause 3 of Section III [*Choice of forum and jurisdiction*].

(c) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

(d) The data importer accepts to abide by a decision binding under the applicable EU / Member State law_.

(e) The data importer agrees that the choice made by the data subject will not prejudice his / her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 7

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any material or non-material damages it causes the other Party/ies by any breach of these Clauses.

---

[8] The data importer may only offer independent dispute resolution through an arbitration body, if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(b)   Liability as between the Parties is limited to actual damage suffered. Punitive damages are excluded.

(c)   Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that Party causes the data subject for any breach of the third party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under the GDPR.

(d)   Where more than one Party is responsible for any damage caused to the data subject resulting from a breach of these Clauses, all responsibleboth Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against either any of these Parties.

(e)   The data importer may not invoke the conduct of a processor (including a sub-processor) to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a)   Each Party shall be liable to the other Party/ies for any material or non-material damages it causes the other Party/ies by any breach of these Clauses.

(b)   Liability as between the Parties is limited to actual damage suffered. Punitive damages are excluded.

(c)   The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject for any breach of the third party beneficiary rights under these Clauses.

(d)   The data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer or its sub-processor causes the data subject for any breach of the third party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under the GDPR.

(e)   Where more than one Party is responsible for any damage caused to the data subject resulting from a breach of these Clauses, all responsibleboth Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against either any of these Parties.

(f)   The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 8

Indemnification

(a)   The Parties agree that if one Party is held jointly and severally liable for a breach of these Clauses together with another Party, it is entitled to claim back as

> **Commented [A130]:** The EDPB and the EDPS recommend the suggested amendment to provide for a more flexible wording for cases where there are more than two parties to the Clauses.

> **Commented [A131]:** Considering this clause will apply in Modules where the data importer is a controller (M1 and M4), the EDPS and the EDPB recommend to add a reference to a 'processor'.

> **Commented [A132]:** The EDPB and the EDPS recommend the suggested amendments to clarify the Clauses and their scope.

> **Commented [A133]:** The EDPB and the EDPS recommend the suggested amendment to provide for a more flexible wording for cases where there are more than one parties to the Clauses.

indemnification that part of the liability that corresponds to the other Party's part of responsibility.

(b)   Indemnification is contingent upon the Party to be indemnified:

   (i)   promptly notifying the other Party of a claim, and

   (ii)   providing reasonable cooperation and assistance to the other Party in defence of such claim.

Clause 9

Supervision

(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 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 cooperate with, 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.

> **Commented [A134]:** For the avoidance of doubt, the EDPB and EDPS would suggest adding a general commitment of the importer to cooperate with the supervisory authority.

SECTION III – FINAL PROVISIONS

Clause 1

Non-compliance with the Clauses and termination

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(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 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 after the suspension,

> **Commented [A135]:** For the sake of clarity, the EDPB and the EDPS recommend this amendment.

(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 non-compliance. 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.

> **Commented [A136]:** The EDPB and the EDPS consider that in case of processor to processor transfers, the controller should also be informed.

> **Commented [A137]:** The EDPB and the EDPS consider that the reference to "responsible Party" needs to be clarified.

(d)   Personal data that has already been transferred prior to the termination of the contract shall [for Modules One, Two and Three: at the choice of the data exporter immediately be returned to the data exporter or destroyed in their entirety. The same shall apply to any copies of the data] [for Module Four: be destroyed in their entirety, including any copy thereof]. The data importer shall ~~certify~~ demonstrate the destruction of the data to the data exporter. These obligations are notwithstanding any requirements under local law applicable to the data importer that prohibits return or destruction of the personal data transferred. In that case, the data importer warrants that it will ensure, to the extent possible, the level of protection required by these Clauses and will only process the data to the extent and for as long as required under that local law.

> **Commented [A138]:** For the avoidance of doubt, the EDPB and the EDPS recommend the suggested amendment.

> **Commented [A139]:** For the avoidance of doubt, the EDPB and the EDPS recommend referring to "without prejudice to".

> **Commented [A140]:** The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.4.1 of the Joint Opinion.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) GDPR that covers the transfer of personal data to which these Clauses apply; or (ii) the GDPR becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under the GDPR.

Clause 2

Governing law

[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 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*).]

Clause 3

Choice of forum and jurisdiction

(a)   Any dispute arising from these Clauses shall be resolved by the courts of a Member State of the European Union. The Parties agree to submit themselves to the jurisdiction of such courts.

(b)   The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c)   Legal proceedings by a data subject against the data exporter and / or data importer may also be brought before the courts of the Member State where the data subject has his / her habitual residence.

ANNEX ₁

*[Please describe **each transfer or category of transfers in a separate Annex** (each consisting of all Parts I to VI). Therefore a separate Annex needs to be signed for each transfer or category of transfers covered by the Clauses.*

Where the Clauses are entered into by more than one data exporter or/and more than one data importer (Multi Party Agreement), each of the parties must complete and sign only those Annex/Annexes (but each of them consisting of Parts I to VI) that relate to the transfer or category of transfers applicable to this party. It is therefore not possible to commonly sign only one Annex for several transfers/sets of transfers, not even if the transfers take place between the same data exporters and data importers.

This is necessary in order to determine, for each transfer/categories of transfers separately, which entity or entities act as data exporter(s) and as data importer(s). Moreover, it needs to be specified, for each transfer/categories of transfers, under Part I of the Annex, if the respective exporter and importer is a controller or a processor as regards the transfer/category of transfers covered by the respective Annex.]

ANNEX, PART I - ~~A~~. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of the data exporter's data protection officer and/or representative in the European Union*]

1. Name: …

Address: …

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

Registration number (if exists):…

Activities relevant to the data transferred under the Clauses: …

Signature and date: …

Role (Controller / Processor)

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: …

Address: …

Registration number (if exists):...

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

Activities relevant to the data transferred under the Clauses: …

Signature and date: …

Role (Controller / Processor)

2. …

[For processor to processor transfers: identity and contact details of the controller(s):

1. Name: …

Address: …

Registration number (if exists):...

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

Activities relevant to the transfer: …

Signature and date: …

2. …]

ANNEX, PART II - ~~B.~~ DESCRIPTION OF THE TRANSFER

[For transfers to (sub-) processors, this annex reflects the corresponding instructions received from the controller(s):]

Categories of data subjects whose personal data is transferred

………………………

Type~~Categories~~ of personal data transferred

………………………

Special categories of personal data transferred (if applicable) and applied restrictions or safeguards that fully takes into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

………………………

Purpose(s) of the data transfer and further processing compatible with this/those purpose(s) (subject matter / description of the processing)

………………………

Type of processing

………………………

Maximum data retention periods, if applicable

………………………

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing and place of storage and processing of data

| | **Commented [A142]:** The EDPB and the EDPS recommend to align the terminology used in the Annex with the terminology used in the Art. 28 GDPR / Art. 29 EUDPR set of SCCs. |

Commented [A142]: The EDPB and the EDPS recommend to align the terminology used in the Annex with the terminology used in the Art. 28 GDPR / Art. 29 EUDPR set of SCCs.

Commented [A143]: The EDPB and the EDPS recommend referring to "type of personal" data rather than "categories of personal data" so it is not understood as only referring to "normal" personal data and special categories of personal data under Article 9 and 10 GDPR.

Commented [A144]: The EDPB and the EDPS recommend referring to "type of processing" in the same way as it is done for binding corporate rules under Article 47(2)(b) GDPR.

Commented [A145]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.2.1 (para. 59) and Section 4.3.3.2 (para. 69) of the Joint Opinion.

Commented [A146]: The EDPB and the EDPS recommend adding this reference to "place and storage and processing of data" so as to ensure consistency with Annex II of the standard contractual clauses between controllers and processors under Article 28(7) GDPR and Article 29(7) EUDPR.

In addition, the EDPB and the EDPS recommend clarifying what does the term "place" mean (e.g. just the country or the exact names and addresses of the facilities where the personal data will be processed?)

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

[Please note:

> *(a) This part of the contract is not subject to the obligation to provide information to data subjects under Articles 13 and/or 14 of the GDPR.*

> *(b) Since a separate Annex (consisting of Parts I to VI) needs to be used **for each transfer or category of transfers** (see Part I), only the specific technical and organisational measures applicable to that transfer/set of transfers at stake be should be indicated here.*

> *(c) The technical and organisational measures need to be described concretely and not merely in a generic manner.]*

[For transfers to (sub-) processors, this annex reflects the corresponding instructions received from the controller(s):]

Description of the technical and organisational measures implemented by the data importer(s), including any relevant certifications

[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 ENSURE AN ADEQUATE THE LEVEL OF SECURITY]

For example:

[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 INDENTIFICATION AND AUTHORISATION]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

Commented [A147]: The EDPB and the EDPS recommend to indicate for clarification that this part of the contract may be redacted if a data subject asks for a copy of these Clauses.

Commented [A148]: For the avoidance of doubt, the EDPB and the EDPS recommend to make this clarification.

Commented [A149]: For the sake of clarity, the EDPB and the EDPS recommend to make this clarification.

[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 [A150]:** The EDPB and the EDPS note that this term is not used in the GDPR. Therefore, the EDPB and the EDPS recommend clarifying or deleting this term.

[DESCRIBE REQUIREMENTS FOR DATA QUALITY]

[DESCRIBE REQUIREMENTS FOR DATA RETENTION]

[DESCRIBE REQUIREMENTS FOR ACCOUNTABILITY]

[DESCRIBE REQUIREMENTS FOR DATA PORTABILITY AND DATA DISPOSAL]

> **Commented [A151]:** The EDPB and the EDPS note that this term is not used in the GDPR. Therefore, the EDPB and the EDPS recommend clarifying or deleting this term.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the data processor to be able to provide assistance to the controller

ANNEX, PART IV - INSTRUCTIONS FROM THE DATA CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA

[to be filled out for transfers "controller to processor" and "processor to processor" only]

ANNEX, PART V – LIST OF SUB-PROCESSORS~~ist of Sub-Processors~~

[to be filled out for transfers "controller to processor" and "processor to processor" only]

The controller has authorised the use of the following subprocessors:

> 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.

ANNEX, PART VI – DOCUMENTATION OF THE MAIN ASPECTS OF THE ASSESSMENT PERFORMED UNDER SECTION II CLAUSE 2 PARAGRAPH b))

[DESCRIBE THE MAIN ASPECTS OF THE ASSESSMENT THAT PERMIT THE PARTIES TO PROVIDE THE WARRANTY IN SECTION II CLAUSE 2 PARAGRAPH a)]

Commented [A152]: The EDPB and the EDPS note that the technical and organisational measures (Annex Part II) seem to be meant as being at the same time the "instructions from the data controller".

However, in the Article 28 / 29 SCCs there is a separate Annex dedicated to the "Instructions from the data controller concerning the processing of personal data".

The EDPB and the EDPS wonder about the reason for this difference. If this means that in these Clauses the "instructions" are identical to the technical and organisational measures, the EDPB and the EDPS would suggest to include an express explanation in this regard.

Otherwise – and preferably - the EDPB and the EDPS would suggest to include a separate annex "Instructions from the data controller concerning the processing of personal data", as in the case of the Article 28 SCCs.

Commented [A153]: For the sake of clarity and in compliance with Clause 4 of Section II, the EDPB and the EDPS recommend specifying that this annex only applies for Module 2 (transfer controller to processor) and Module 3 (transfer processor to processor).

Commented [A154]: The EDPB and the EDPS invite the Commission to refer to the corresponding comments made in Section 4.5 of the Joint Opinion.

Commented [A155]: The EDPB and the EDPS recommend clarifying what does the term "place" mean (e.g. just the country or the exact names and addresses of the facilities where the personal data will be processed?)

Commented [A156]: The EDPB and the EDPS invite the Commission to refer to the corresponding comment made in Section 4.3.6.2 of the Joint Opinion.