Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR)

Adopted on 9 July 2019

1 CONTENTS

The European Data Protection Board

Having regard to Article 28(8), Article 63 and Article 64(1)(d), (3) - (8) of the Regulation 2016/679/EU 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 (hereafter "GDPR"),

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]

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the Board) is to ensure the consistent application of the GDPR throughout the European Economic Area. To this effect, it follows from Article 64(1)(d) GDPR that the Board shall issue an opinion where a supervisory authority (SA) aims to determine standard contractual clauses (SCCs) pursuant to Article 28(8) GDPR. The aim of this opinion is therefore to contribute to a harmonised approach concerning cross border processing or processing which can affect the free flow of personal data or natural person across the European Economic Area and the consistent implementation of the GDPR's specific provisions.

(2) In the context of the relationship between a data controller and a data processor, or data processors, for the processing of personal data, the GDPR establishes, in its Article 28, a set of provisions with respect to the setting up a specific contract between the parties involved and mandatory provisions that should be incorporated in it.

(3) According to Article 28(3) GDPR, the processing by a data 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.

(4) Under Article 28(6) GDPR, without prejudice to an individual contract between the data controller and the data 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).

(5) Furthermore, Article 28(8) GDPR determines that a SA may adopt a set of standard contractual clauses in accordance with the consistency mechanism referred to in Article 63. That is to mean that SAs are required to cooperate with other members of the Board and, where relevant, with the European Commission through the consistency mechanism. SAs are required, pursuant to Article 64(1)(d) to communicate to the Board any draft decision aiming to determine standard contractual clauses pursuant to Article 28(8). In this context, the Board is required to issue an opinion on the matter, pursuant to Article 64(3), where it has not already done so.

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

(6) 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.

HAS ADOPTED THE OPINION:

2 SUMMARY OF THE FACTS

1. The competent supervisory authority of Denmark has submitted its draft standard contractual clauses (hereafter SCCs) to the Board via the IMI system requesting an opinion from the Board pursuant to Article 64(1)(d) for a consistent approach at Union level. The decision on the completeness of the file was taken on the 4th of April 2019. The Board Secretariat circulated the file to all members on behalf of the Chair on the 4th of April.

2. The Board has received the draft SCCs from the Danish SA[2] along with a letter explaining the structure of the standard contractual clauses. These two documents were provided by the Danish SA in an English version. The Board hereby gives its opinion on the English version of the document although the Board notes that the SCCs is also available in Danish on the website of the Danish SA. The Danish SA shall take utmost account of the opinion of the Board.

3. In compliance with Article 10(2) of the Board Rules of Procedure[3], due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks (until the 9th of July 2019).

[2] "Data Processing agreement" is the term used by the Danish SA in the document provided to the Board to refer to Standard Contractual Clauses.
[3] Version 2, as last modified and adopted on 23 November 2018.

3 ASSESSMENT

3.1 General reasoning of the Board regarding the set of standard contractual clauses

4. Any set of standard contractual clauses submitted to the Board must further specify the provisions foreseen in Article 28 GDPR. The opinion of the Board aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented draft clauses that could serve as standard contractual clauses in compliance with Article 28(8) GDPR.

5. The Board notes that that the document presented to the Board is a draft SCCs containing two parts:

    1) a general part containing general provisions to be used as is; and

    2) a specific part that has to be completed by the parties with regard to the specific processing which the contract seeks to govern.

6. In addition, the Danish SA explains, in its letter, that the clauses of the SCCs which are in bold are mandatory and constitute the minimum requirements of a contract under Article 28 GDPR. The remaining clauses, although advisable to include in a SCCs, are voluntary and may be included in the SCCs at the discretion of the parties.

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

8. When this opinion remains silent on one or more clauses of the SCCs submitted by the Danish SA, it means that the Board is not asking the Danish SA to take further action with regards to this specific clause. Clauses 6.4, 9.3 and 14.3 of the Danish SCCs are not required by article 28 and are related to commercial aspects and the Board therefore does not see these clauses as being part of the SCCs. It is up to the Parties whether, and how, to enter into agreement.

3.2 Analysis of the draft standard contractual clauses

3.2.1 General remark on the whole SCCs

9. The Board is of the opinion that if the SCCs only contained the sections in bold, it would not be sufficient as SCCs, since some of the non-bold sections relate to mandatory provisions under Article 28(3) GDPR. Therefore, the Board recommends that the Danish SA avoid this distinction by clearly stating, either in the clauses or in a separate document instructing on the use of these clauses, that all clauses of the SCCs together with the appendices should be included in the SCCs concluded by the parties.

10. In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority do not prevent the parties from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the adopted standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Furthermore, where the standard data protection clauses are modified, the parties will no longer be deemed to have implemented adopted standard contractual clauses.

11. The Board notes that the wording of several clauses of the SCCs are not in line with to the relevant provisions of the GDPR. The Board has indicated this in its opinion below and recommends that the Danish SA align the wording of those clauses with the relevant provisions of the GDPR.

3.2.2 Data Processing Preamble (Clause 2 of the SCCs)

12. Regarding **clause 2.3** of the SCCs, the Board is of the opinion that the relationship between the data processing agreement and the "master agreement" could be more flexible. There may be cases where the standard contractual clauses are a distinct document part of the master agreement and as such, there is no need for distinct SCCs. There may also be situations where the data processing governed by the SCCs is not part of a master agreement. The Board therefore encourages the Danish SA to redraft this clause to reflect this flexibility. This specific change needs to be implemented in each occasion where the SCCs refers to the master agreement.

13. Regarding **clause 2.4** of the SCCs, first sentence, the Board is of the opinion that in some situations, the data processing agreement might be terminated before the "main agreement". The Board recommends that the Danish SA adds, at the end of the first sentence, that the agreement "*cannot, in principle, be terminated separately, except where the data processing ends before the termination of the master agreement, or where other conditions for separate termination of the standard contractual clauses, as specified under its termination clauses, are met (see also recommendation on clause 14.4 below)*".

3.2.3 The rights and obligations of the data controller (Clause 3 of the SCCs)

14. Regarding **clause 3.1** of the SCCs, the Board is of the opinion that the wording "*shall be responsible to the outside world*" is misleading. Indeed, it could be understood as placing obligations towards data subjects or other stakeholders solely on the data controller. The Board is of the opinion that this clause would be clearer if a reference to Article 24 GDPR and its accountability principle is made. The Board subsequently recommends that the Danish SA adds such a reference.

15. Further, regarding the clause 3.1, it would be better to refer, in general, to the applicable legislation in data protection matter, where relevant, instead of to a specific act. The Board recommends that the Danish SA amend the reference to the Data Protection Act. Finally, the Board suggests replacing the words "in the framework of" by "in compliance with".

    Therefore the Board would suggest the following wording as an example:

    "1. *The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the General Data Protection Regulation (see Article 24 GDPR), the applicable EU or Member States data protection provisions () and this standard contractual clauses*."

16. Regarding **clause 3.2** of the SCCS, the Board is of the opinion that this clause is unclear, since the data controller has already defined the purposes and means of the processing activity subject to the SCCs. The Board recommends the Danish SA to modify this clause as follows:

17. "*The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data*".

18. Regarding **clause 3.3** of the SCCs, the Board is of the opinion that its meaning is unclear. The Board assumes that the idea behind this clause is to make sure that the processing activities for which the data controller wishes to engage a data processor have a legal basis. If it is the case, the Board recommends that the Danish SA clarifies the clause accordingly.

Finally, the Board notes that in clause 3.1 of the SCCs the wording "processing of personal data" is used. In clause 3.3 of the SCCs, the word "processing" is used. The Board recommends that the Danish SA use the same terminology in order to avoid confusion.

As an example, the Board would therefore suggest the following wording:

"3. *The data controller shall be responsible, among others, for ensuring that the processing of personal data which the data processor is instructed to perform has a legal basis*."

3.2.4 The data processor acts according to instructions (Clause 4 of the SCCs)

19. Regarding **clause 4.1** of the SCCs, the Board is of the opinion that a reference should be made to appendices A and C as they further specify the data controller's instructions. The Board is of the opinion that additional instructions can be given by the data controller throughout the duration of the contract but such instructions shall always be documented.

    Further, the Board notes that this clause is inspired by Article 28(3)(a) GDPR. The Board would therefore encourage the Danish SA to use the same wording as in the GDPR.

20. Regarding **clause 4.2** of the SCCs, the Board is of the opinion that in case of unlawful instructions, parties should foresee consequences and provide solutions.

3.2.5 Confidentiality (Clause 5 of the SCCs)

21. The Board understands clause 5 of the SCCs as the specification of Article 28(3)(b) GDPR which states that "*the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality*".

22. Regarding **clause 5.1** of the SCCs, the word "currently" is understood by the Board as the necessity to keep the status of "authorised persons" under review. Further, it is unclear to the Board who is giving the authorisation to those persons in particular since access to personal data has to be provided on a "need-to-know" basis.

23. Regarding **clause 5.2** of the SCCs, the Board is of the opinion that this clause relates to the principle of the access to the personal data on a "need-to-know" basis. The Board is of the opinion that clauses 5.1 and 5.2 of the SCCs can be combined as follows:

    "*It is the responsibility of the data processor to grant access to persons under its authority to the personal data being processed on behalf of the data controller only on a need to know basis and who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The list of persons to whom access has been granted needs to be kept under periodic review. On the basis of the said review, access to personal data can be withdrawn and in this case, personal data cannot be accessible anymore to those persons.*"

24. Regarding **clause 5.3** of the SCCs, the Board is of the opinion that it is covered by the suggested wording above and clause 5.3 can therefore be deleted.

25. Regarding **clause 5.4** of the SCCs, the Board recommends that the Danish SA delete the wording "*be able to*" since the data processor has to demonstrate compliance with the confidentiality requirements. Further, the Board encourages the Danish SA to adopt a broader wording when referencing to "*employees*" as there may be other persons than employees processing personal data

under the authority of the processor. Wording such as "*person under the authority of the processor*" or "*persons employed directly or indirectly by*" would be more appropriate.

3.2.6 Security of processing (Clause 6 of the SCCs)

26. Regarding **clause 6.1** of the SCCs, the Board recommends that the Danish SA replace the words "*with consideration for the current level*" in the beginning of the sentence by the words "taking into account the state of the art", which is the wording of Article 32(1) GDPR. This specific wording is used in the GDPR to make sure that the level of security applied to the processing of personal data is always in line with the latest technological evolutions. The wording suggested by the Danish SA makes reference to a current level which will not be the state of the art in 2 years.

27. Regarding **clause 6.2** of the SCCs, the Board understands that this provision relates to Article 28(3)(c) of the GDPR and that clause 9.2 relates to Article 28(3)(f) of the GDPR. However, the distinction between the two clauses and the different tasks of the data processor in not very clear. The Board recalls that Article 28(3)(f) GDPR states that the data processor assists the data controller in ensuring compliance with the obligations under Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the data processor.

The Board is of the opinion that the "risk assessment" referred to in the first sentence of clause 6.2 has to be performed on the processing activities, which the data controller will entrust to the data processor. The data controller should therefore provide the data processor with all the information necessary so that the data processor can comply with Article 28(3)(c) and (f) of the GDPR. The Board would like to emphasize that this does not exempt the data controller from the responsibility to be in compliance with its own obligations under Article 25, 32 or 35-36 GDPR.

In addition, the end of the first sentence of clause 6.2 needs to be redrafted in order to be more in line with clause 9.2 and appendix C2 as it is not clear for the Board how the wording "*thereafter implement measures to counter the identified risk*" in clause 6.2 is related to clause 9.2 and appendix C2. The Board has noticed that clause 9.2.a and appendix C2 address the topic of risk assessment but not in the same way as clause 6.2. Under clause 6.2, the risk assessment is to be performed by the data processor, whereas under clause 9.2 and appendix C2, the risk assessment is to be performed by the data controller. Appendix C2 further sets out that the data processor shall implement measures that have been agreed with the data controller.

Regarding appendix C2, the Board is of the opinion that the wording "*The level of security shall reflect" could be changed into* "*The level of security shall take into account*". Regarding the elements to be taken into account, Articles 32(1) and 32(2) GDPR mentions the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons. These could be elements to mention in order to clarify what is expected by "*Describe elements that are essentials to the level of security*".

Therefore, the Board recommends that the Danish SA clarifies and aligns clauses 6.2, 9.2 and Appendix C2.

3.2.7 Use of Sub-Processors (Clause 7 of the SCCs)

28. Regarding **clauses 7.2 and 7.5** of the SCCs, the Board recommends that the Danish SA replace the word "consent" by "authorisation", as this is the wording of Article 28(2) GDPR.

Furthermore, the Board is of the opinion that it would be more practical to create options in this clause as follows:

"2. *The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of these standard contractual clauses without the prior [Choice 1] specific authorisation of the data controller / [Choice 2] general written authorisation of the data controller*."

29. Regarding **clauses 7.3 and 7.4** of the SCCs, the Board finds it important to add the fact that the list of sub-processors which are accepted by the data controller at the time of the signature of the contract should be included as an appendix to the SCCs, be it on the basis of a general authorisation or a specific one. The purpose of this list is to ensure that even in cases of a general authorization, the data controller remains informed about the list of sub-processors as well as further changes. The Board recommends that the SCC clarifies that the list of sub-processors in appendix B2 has to be provided both in cases of general and specific prior authorisation.

Further, in appendix B1 of the SCCs, there are examples of clauses that the parties can choose in-between. The Board considers that it would, however, be better to included such clauses in the SCCs itself instead of in the appendices.

Finally, as regards the general prior authorisation, the Board is of the opinion that any conditions that the data processor might set for the data controller to object to changes of sub-processor(s) must allow the data controller to, in practice, exercise its freedom of choice and enable the data controller to remain in control over the personal data. This implies also that the data controller should have sufficient time to object to such a change.

The Board recommends that the Danish SA redraft clause 7.3 to create options within the clause that can be chosen by the parties within the SCCs and to incorporate the content of clauses 7.4 and 7.5 within 7.3.

Clause 7.3 could be drafted as follow:

"*3. In case of general written authorisation, the data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors in at least [specify time period], and thereby giving the data controller the opportunity to object to such changes prior to the engagement of any sub-processor. Longer time periods of prior notice for specific sub-processing services can be provided in the Appendix B. The list of sub-processors already accepted by the data controller can be find in appendix B."*

In case of specific prior authorisation, the data processor shall engage sub-processor solely with the prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least [specify time period] prior to the engagement of any sub-processor. The list of sub-processors already accepted by the data controller can be found in appendix B."

As the option is created in the draft SCCs itself, appendix B1 can be deleted. In addition, the Board recommends that the Danish SA adds a possibility to have a longer period of prior notice in appendix B.

30. Regarding **clause 7.6** of the SCCs, the Board understands this clause as a reference to Article 28(4) GDPR. As previously mentioned, it would be better to refer to the exact wording of the text of the GDPR to avoid any confusion.

Regarding **clause 7.8** of the SCCs, the Board would like to underline the fact that its content is not required by Article 28 GDPR. The Board is of the opinion that the words "third party" are unclear. If

the intention is to create a "third party beneficiary right" for the data controller within the contract between the data processor and the sub-processor, this should be specified.

As such, the Board sees an added value in having such a clause as part of a standard contractual clauses. Indeed, it preserves the rights of the data controller, including liability. For this reason, the Board encourages the Danish SA to make it clearer that the intention is to create a third beneficiary right for the data controller. This would imply for instance that the sub-processor would accept to be liable to the data controller in case of the initial data processor is bankrupt or the possibility for the controller to directly order the sub-processor to return the data.

31. Regarding **clause 7.9** of the SCCs, the Board is of the opinion that it is important to make a reference to the rights of the data subject. This reference can be made as follows: "*This does not affect the rights of the data subjects under the GDPR - in particular those foreseen in Articles 79 and 82 GDPR - against the data controller and the data processor, including the sub-processor*."

3.2.8 Transfer of data to third countries or international organisations (Clause 8 of the SCCs)

32. Regarding the title of the clause, the Board is of the opinion that it should be clarified that the words "third countries" refers to countries outside of the EEA and not outside of Denmark. The Board encourages the Danish SA to clarify this.

33. The Board is of the opinion that section 8 should clarify that the data controller has to decide whether a transfer is allowed under the contract or if it should be prohibited. The Board recommends to the Danish SA that this is made clear in the standard contractual clauses and encourages it to specify this in appendix C5.

34. Regarding **clause 8.1** of the SCCs, the Board notes that the Danish SA has added parentheses after the word "transfer" as following "(assignment, disclosure and internal use)". The Board wonders whether this aims at giving a definition of the word "transfer". If this is the intention, the Board is of the opinion that as there is no such definition of the notion of transfer in the GDPR, it is better to delete these terms in parentheses.

Finally, the Board recommends that the Danish SA start its clause 8.1 by adding "*In compliance with Chapter V GDPR* ..." Indeed, the Board recalls that for any transfer outside of the EU, all provisions of Chapter V GDPR need to be complied with. It should be clarified under clause 8 that these SCCs cannot be understood as SCCs fulfilling the requirements of Art. 46 GDPR and therefore cannot be used as a tool to carry out international transfers within the meaning of Chapter V of the GDPR. This could be in addition reflected in the title of clause 8, which otherwise may give the impression that transfers can be carried out on the basis of these SCCs.

35. Regarding **clause 8.2** of the SCCs, the Board has several remarks.

First, in the beginning of the sentence, the Board encourages the Danish SA to add the word "documented" before "instructions" to ensure legal certainty and alignment with Article 28(3)(a) GDPR and to change the word "*approval*" to "*authorisation*" in line with the terms used under Article 28 GDPR. The beginning of the sentence should be "*Without the documented instructions or authorisation of the data controller*".

Second, on clause 8.2.a, the word "*disclose*" might create confusion with the notion of transfer. In addition, personal data can be transferred to a data controller (as already mentioned in the clause) but also to a data processor in a third country. The Board recommends that the Danish SA drafts clause

8.2.a as follows: "*transfer personal data to a data controller or a data processor in a third country or in an international organisation*".

Third, on clause 8.2.b, the word "assign" might also create confusion with the notion of transfer. The Board recommends that Danish SA replace the word "assign" by the word "transfer".

Finally, on clause 8.2.c, it is unclear to the Board what the meaning of the word "divisions" is. The Board encourages the Danish SA to replace clause 8.2.c by the following sentence: "*have the data processed by the Data Processor outside the EEA*".

36. Regarding **clause 8.3** of the SCCs, the Board understands that it is a way to have the instructions of the data controller documented in the appendix C5. As already stated in the beginning of its opinion, the Board sees the appendices as mandatory. However, the Board is of the opinion that mentioning the choice of the tool for transfer could have a benefit, in addition to the instructions as it contributes demonstrating compliance of the parties with Chapter V of the GDPR. The Board encourages the Danish SA to amend clause 8.3 as follow:

37. "*The data controller's instructions regarding transfers of personal data to a third country including, if applicable, the transfer tool on which they are based, shall be set out in appendix C5 of these standard contractual clauses. The same procedure shall be applied for the approval of transfers of personal data to a third country*."

3.2.9 Assistance to the data controller (Clause 9 of the SCCs)

38. **Clause 9.1** of the SCCs reflects the content of Article 28(3)(e) of the GDPR. The obligation of the data processor under this clause is to assist the data controller to respond to requests for exercising data subject's rights. The assistance can take various forms. The Board is of the opinion that the SCCs needs to give details on the manner in which the processor is required to provide assistance and not only the list of possible rights to be exercised.

Notably, the SCCs should set out the steps to be taken by the data processor in case the latter directly receives a request from a data subject relating to the exercise of his/her rights. For example, it has to be clear in the agreement in such a case as to whether the data processor is not allowed to have any contact with the data subjects, and how the processor needs to inform the controller when it comes to data subjects' rights (e.g. forwarding the request to the controller within a specified timeframe or other appropriate measures). In this case, the assistance is provided only through an exchange of information between the data controller and the data processor. Another scenario could be that the data controller instructs the data processor to answer to data subject's requests according to instructions given. Another option could be that the data processor would make the technical implementations instructed by the data controller with respect to data subject rights. The Board recommends that the Danish SA reflect on the possibility to include the following sentence under clause 9.1 of the SCCs:

"*The parties shall define in appendix C the appropriate technical and organisational measures with which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in clauses 9.1 and 9.2 of the standard contractual clauses."*

A new point in appendix C needs to be created in order to have the technical and organisational measures specified.

Further, on clause 9.1.a and 9.1.b the Board recommends that the Danish SA use the words "*right to be informed*" instead of the word "*notification*", as follow: "*Right to be informed when collecting personal data from the data subject*" - "*Right to be informed when personal data have not been obtained from the data subject".*

Regarding clause 9.1.j, the Board would prefer to have the exact wording of the GDPR. The Board therefore encourages the Danish SA to redraft it as follow "*the right not to be subject to a decision solely based on automated processing, including profiling*".

39. **Clause 9.2** of the SCCs reflects the content of Article 28(3)(f) of the GDPR. Hence the Board recommends replacing "*data made available*" by "*information available*". The obligation of the data processor under this clause is to assist the data controller for the fulfilment of the legal duties relating to the security, the data protection impact assessment and prior consultation of SAs. Here again, the Board is of the opinion that the SCCs needs to give details on the manner in which the data processor is required to provide assistance to the data controller.

As already stated in paragraph 27 of this opinion, the Danish SA should clarify the relationship between clause 9.2 and clause 6 on security of the processing. The Board understands the relationship between those two clauses as referring to Article 28(3)(c) of the GDPR for clause 6 and to Article 28(3)(f) for clause 9.2. Indeed, clause 9.2.a and to a certain extent clause 9.2.b are obligations that need to be fulfilled in all cases by the data processor subject to the GDPR. This follows from Article 32(1) and Article 33(2) GDPR. For clause 9.2.a to be kept, some further alignments with Article 32(1) GDPR would be required. The Board recommends to the Danish SA to make clear that the risk would be the risk "for the rights and freedoms of natural persons". Furthermore, not only is the nature of the processing to be taken into account, but also the state of the art, the costs of implementation, the scope, the context and the purposes of the processing. The Board understands that the parties should specify in Appendix C2 the minimum level of security and measures to be implemented by the data processor. The Board considers it important that details on assistance to the data controller as regards security of the processing be included in the instructions under appendix C2.

The Board has provided a drafting suggestion covering clauses 9.1 and 9.2 above.

On clause 9.2.b, the Board is of the opinion that any reference to a specific national supervisory authority in a model contract should be avoided. In addition, the words "*report*" should be replaced by "*notify*" and "*discovering*" should be replaced by "*after becoming aware*" to be in line with Article 33(2) GDPR.

Clause 9.2.b could be drafted as follow: "b. *its obligation, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, to report personal data breaches to the competent supervisory authority, [PLEASE INDICATE the competent SA], without undue delay and where feasible, no later than 72 hours after having become aware of such breach*".

On clause 9.2.e, here again, the Board is of the opinion that the reference to the Danish SA should be removed. Clause 9.2.e could be drafted as follow: "*e. the obligation to consult the competent supervisory authority, [PLEASE INDICATE the competent SA], 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*".

The Board considers important to have this clause further detailed in appendix C or D to ensure that the parties make arrangements on the manner this assistance will be provided in practice.

3.2.10 Notification of personal data breach (Clause 10 of the SCCs)

40. Regarding **clause 10.1** of the SCCs, the Board, as already stated, favours the wording of the GDPR in order to avoid any confusion. In this clause, the word "discovery" should be changed into "after having become aware". In addition, the Board encourages the Danish SA to add the word "any" before personal data breach in order to make clear that it is not up to the data processor to assess whether or not the data breach has to be notified to the competent SA. This is the data controller's responsibility[4].

The sentence could be changed as follow: "1. *In case of any personal data breach, the data processor or sub-processor shall, without undue delay after having become aware of it, notify the data controller*."

The Board recommends deleting "*at the data processor's facilities or a sub-processor's facilities*" which would limit the notification obligation to cases where the breach occurs in these facilities, whereas such limitation does not stem from the GDPR.

Regarding the second part of clause 10.1, the Board is of the opinion that it can be completed as follows:

"*The data processor's notification to the data controller shall, if possible, take place with-in [number of hours] after the data processor has become aware of the breach in order to enable the data controller to comply with his obligation to report personal data breaches already mentioned in clause 9.2.b. "*

41. Regarding **clause 10.2** of the SCCs, the Board is of the opinion that the words "*taking into account the nature of the processing and information available*" could be further specified in appendix D in order to be more concrete and tailor-made. The following wording could be added in a new paragraph at the end of clause 10.2:

"*The parties shall define in appendix D the elements to be provided by the data processor to assist the data controller in the reporting of a breach to the supervisory authority."*

In addition, in the beginning of the second sentence of clause 10.2, the draft SCCs states "*This may mean - on the basis of the information available to the Processor - (...)*". The Board is of the opinion that - for the sake of legal certainty - it is better to avoid this kind of formulation. The Board encourages the Danish SA to amend this wording by deleting the word "*may*".

3.2.11 Erasure and return of data (Clause 11 of the SCCs)

42. Regarding **clause 11** of the SCCs, the Board is of the opinion that it would be more practical to create a real option in this clause. The Board encourages the Danish SA to amend this clause in order to create two concrete options to be chosen by the Data Controller.

The clause could be drafted as follows:

[4] See Guidelines on data breach notification (p. 13) "It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller."

"On termination of the processing services, the data processor shall be under obligation [Option 1] *to delete all personal data processed on behalf of the data controller* [Option 2] *to return all the personal data to the Data Controller and to erase existing copies.*

[Optional] *The following EU or Member states law applicable to the processor requires storage of the personal data after the termination of the processing services*: ..... The *processor commits to exclusively process the data for the purposes provided by this law and under the strict applicable conditions.*"

More information could be provided in the appendix C3, including the possibility for the data controller to modify the option chosen at the signature of the contract. This, as a consequence, affects the content of appendix C3. The Board encourages the Danish SA to better distinguish the storage period from the erasure procedures under appendix C3 and to reflect the possibility for the data controller to change the choice made.

Finally, the Board is of the opinion that the words "processing services" need to be specified for instance by "after the end of the provision of services relating to processing". This can be done in the appendix D.

3.2.12 Inspection and audit (Clause 12 of the SCCs)

43. **Clause 12.1** of the SCCs reflects the content of Article 28(3)(h) of the GDPR. The Board recommends to use the same terminology of paragraph 1 "audits, including inspections" within paragraphs 2 and 3 which only refer to inspection.

44. Regarding **clause 12.3** of the SCCs, the Board understands it as covering audit and inspections towards the sub-processor. In accordance with Article 28(4) of the GDPR, the same obligations as set out in the contract or another legal act between the controller and the processor shall be imposed on the sub-processor. This includes the obligation under Art. 28(3)(h) to allow for and contribute to audits by the data controller or another auditor mandated by the data controller. The drafting of clause 12.3 seems to limit this right of the data controller vis-a-vis the sub-processor ("if applicable" and "performed through the Data processor"). The Board recommends that the Danish SA redrafts clause 12.3 in order to be in full compliance with the GDPR. This can be done by merging clauses 12.2 and 12.3 as follows: "*Procedures applicable to the data controller's audits, including inspections of the data processor and the data sub-processor are specified in* appendices C6 and C7 *to these standard contractual clauses.*"

45. Regarding appendices C6 and C7, the Board recommends the Danish SA to change the following sentence "*The inspection report shall without delay be submitted to the Data Controller for information purposes*" to make it clear that the controller is be able to contest the scope, methodology and the results of the inspection. The controller should also be able to request measures to be taken following the results of the inspection.

46. In addition, the reference is appendix C6 to "*Data Processor's facilities*" and C7 to "*Sub-Processor's facilities*" need to be broaden. Indeed, rights of the data controller in the framework of inspections and/or audit should not be limited to the facilities of the processor or sub-processors. The data controller should have access to the places where the processing is being carried out. This includes physical facilities as well as systems used for and related to the processing.

3.2.13 The parties' agreement on other terms (Clause 13 of the SCCs)

47. Regarding **clause 13** of the SCCs, the Board recommends that the Danish SA bear in mind that if a paragraph specifying liability, governing law, jurisdiction or other terms is included, it cannot lead to any contradiction with the relevant provisions of the GDPR or undermine the level of protection offered by the GDPR or the contract.

3.2.14 Commencement and termination (Clause 14 of the SCCs)

48. Regarding **clause 14.4** of the SCCs, the Board is of the opinion that a specific provision on the termination of the contract might also be relevant for the SCCs. As the position of the Board is that the relationship between the data processing agreement and the master agreement should be more flexible, the Board recommends that the Danish SA includes a provision on the termination within the SCCs.

49. Regarding **clause 14.5** of the SCCs, the Board is of the opinion that this clause might be in contradiction with clauses 2.4 or 14.4. The Board recommends that the Danish SA clarifies the relationship between those three clauses.

3.2.15 Appendix A

50. Appendix A aims at giving details about the processing activities undertaken by the data processor on behalf of the data controller. To this end, the Board recommends that the purpose and the nature of the processing are described, as well as the type of personal data processed, the categories of data subjects concerned and the duration of the processing. This 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 as defined in article 4(1)" or stating which category (Article 6, 9 or 10) of personal data is subject to processing. The Board is of the opinion that it should be clear that in case of several processing activities, these elements have to be completed for each of them. In addition, the Board is not convinced by the two first examples, as it is difficult to distinguish the purpose to the nature of the processing.

4 CONCLUSIONS

51. The Board very much welcomes the Danish initiative to submit their draft SCCs for an opinion which aim at contributing to an harmonized implementation of the GDPR.

52. The Board is of the opinion that the draft SCCs of the Danish Supervisory Authority submitted for an opinion need further adjustments in order to be considered as standard contractual clauses. The Board made several recommendations in its opinion here above. If all recommendations are implemented, the Danish SA will be able to use this draft agreement as Standard Contractual Clauses pursuant to article 28.8 GDPR without any need for a subsequent adoption from the EU Commission.

5 FINAL REMARKS

53. This opinion is addressed to Datatilsynet (the Danish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

54. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft SCCs. Within the same period, it shall provide the amended draft SCCs[5] or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[5] The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.