Opinion of the Board (Art. 64)

Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR)

Adopted on 19 May 2020

TABLE OF 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 (hereinafter, "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 (hereinafter, the "Board") is to ensure the consistent application of the GDPR throughout the Union. To this end, the Board shall issue an opinion based on Article 64(1)(d) GDPR where a supervisory authority (hereinafter, "SA") aims to determine standard contractual clauses (hereinafter, also "SCCs") referred to in Article 28(8) GDPR. The aim of this Opinion is therefore to contribute to a harmonised approach concerning measures to be adopted by a supervisory authority that are intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States 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 of a specific contract between the parties involved and to 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*"; a set of specific aspects to regulate the contractual relationship between the parties is therefore set out, including among others, the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects.

(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, in whole or in part, on standard contractual clauses. These standard contractual clauses are to be adopted for the 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. In this regard, SAs are required to cooperate with other members of the Board and, where relevant, with the European Commission through the consistency mechanism. Pursuant to Article 64(1)(d), SAs are required to communicate to the Board any draft decision aiming to determine standard contractual clauses

[1] References to the "Union" made throughout this Opinion should be understood as references to the "EEA".

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 issued an opinion on the same matter.

(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.

(7) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Slovenian supervisory authority (hereinafter, “SI SA”) has submitted its draft decision and its draft standard contractual clauses to the Board, requesting its opinion pursuant to Article 64(1)(d), for a consistent approach at Union level. The decision on the completeness of the file was taken on 21 February 2020. The EDPB Secretariat circulated the file to all members on behalf of the Chair on 21 February 2020.

2. The Board has received the draft SCCs from the SI SA along with a draft decision explaining the background and structure of the standard contractual clauses. These two documents were provided by the Slovenian SA in an English version.

3. In compliance with Article 10(2) of the Board Rules of Procedure[2], 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 29 May 2020).

2 ASSESSMENT

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

4. Any set of standard contractual clauses submitted to the Board under Article 28(8) and Article 64(1)(d) 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, which could serve as Art. 28(8) standard contractual clauses.

5. The Board notes that the draft SCCs presented to the Board are composed of two parts:

[2] Version 6, as last modified and adopted on 29 January 2020.

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 SI SA explains, in its draft decision, that the model contract (SCCs) "addresses the main issues that are frequently discussed by the controllers and processors when determining their mutual rights and obligations", and that more specifically it "primarily addresses the content, set out in Article 28(3) GDPR" but it "also addresses issues that can, in line with [their] experience, cause uncertainty among the parties and need special attention".

7. Among the elements to be taken into account by the Board, the SI SA specified to the EDPB members in its request that it followed the example of the SCCs submitted by the Danish SA[3] and considered Opinion 14/2019 of the EDPB, adopted on 9 July 2019 by the EDPB[4]. The Board recognises that the SI SA has taken into account the referred Opinion already adopted by the Board on draft SCCs for the purposes of compliance with Article 28 GDPR and recalls that the evaluation of each draft decision subject to the consistency mechanism is made individually and on its own merits, bearing in mind the goal of ensuring consistency.

8. When this opinion remains silent on one or more clauses of the SCCs submitted by the SI SA, it means that the Board is not asking the SI SA to take further action with regard to those specific clauses.

2.2 Analysis of the draft standard contractual clauses

2.2.1 General remark on the whole SCCs

9. Since a contract under Article 28 GDPR should further stipulate and clarify how the obligations in Article 28(3)-(4) will be fulfilled, the SCCs need to be analysed in their entirety.

10. In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority does 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.

2.2.2 Preamble (Clause 1 of the SCCs)

11. Regarding **clause 1.5** of the SCCs, the Board notes that other goals are also pursued through standard contractual clauses adopted for the purpose of Article 28. Thus, the Board encourages the SI SA to rephrase the sentence as follows: "*The Clauses are intended to protect the rights of the data subjects, mitigate specific data protection risks and ensure clarity in the relationship between the controller and the processor and as to the respective rights and duties*".

[3] The final version of the standard contractual clauses for the purposes of compliance with Article 28 GDPR adopted by the Danish SA is available here: https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses-purposes-compliance-art_en.

[4] EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), adopted on 9 July 2019, available here: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf.

2.2.3 The data processor acts according to instructions (Clause 3 of the SCCs)

12. Regarding **clause 3.1** of the SCCs, the Board encourages the SI SA to add the word "or" in "Union [or] Member State law".

13. The SCCs specify in **clause 3.3** that "*[t]he data processor and, where applicable, the processor's representative will in accordance with Article 30(2) GDPR maintain a record of all categories of processing activities carried out on behalf of a controller*". While Article 28(3) GDPR does not specifically impose on controllers and processor a duty to include in the contract the obligation for the processor to keep a record under Article 30(2) GDPR, the Board considers this measure as contributing "to demonstrate compliance" and helpful to "assist the controller in ensuring compliance with the obligations pursuant to Article 32 to 36" (Article 28(3)(h) and (f) GDPR).

2.2.4 Confidentiality (Clause 4 of the SCCs)

14. The Board understands that **clause 4.2** of the SCCs refers to the possibility for the controller to ask the processor to demonstrate that the persons under the processor's authority who have access to the personal data are bound by an obligation of confidentiality and their access to personal data is only granted on a need-to-know basis. Consequently, the Board encourages the SI SA to slightly rephrase the clause in order to clarify it. For instance, the clause could be redrafted as follows: "*The data processor shall, at the request of the data controller, demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned obligation of confidentiality and are only given access to personal data on a need-to-know basis*".

2.2.5 Security of processing (Clause 5 of the SCCs and Appendix C.2)

15. With regard to **clause 5.1** of the SCCs, the Board would like to highlight that it is generally not appropriate for standard contractual clauses to merely restate the content of the provisions of the GDPR as they should rather specify the concrete application of relevant obligations. Although this clause is not considered as problematic, the EDPB encourages the SI SA to slightly rephrase it (e.g. "*Pursuant to Article 32 GDPR, which stipulates that [...], the parties shall implement [...]*").

16. With regard to **clause 5.3**[5] of the SCCs, the Board understands it as referring to a risk assessment independently performed by the processor in order to comply with Article 32 and Recital 83 GDPR. The Board encourages the SI SA to clarify that such assessment refers to the processing entrusted to the processor by the controller and recalls that the controller is anyway not exempt from its obligations to comply with Articles 25, 32, 35, 36 GDPR. For instance, clause 5.3 could be rephrased as follows: "*According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the controller, and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks*".

[5] The draft clause 5.3 specifies: "*According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks*".

17. **Appendix C.2** invites the parties to list the security measures that have been agreed by the parties and need to be implemented by the data processor. The Board recalls that the degree of detail of this information must be such as to enable the controller to assess the appropriateness of the measures and to comply with its obligation of accountability.

2.2.6 Transfer of data to third countries or international organisations (Clause 7 and Appendix C.6 of the SCCs)

18. The Board encourages the SI SA to clarify that the words “third countries” refer to countries outside of the EEA and not outside of Slovenia. This could be carried out by adding in clause 7.1 *“[...] third countries (i.e. countries outside of the European Economic Area) [...]”*.

19. With regard to **clause 7.3** of the SCCs, the Board encourages the SI SA to specify that the reference to the “authorisation” of the controller is not an alternative to the “documented instructions” but rather describes a possible content of such instructions. Additionally, the Board encourages the SI SA to further clarify the relationship among clauses 7.1, 7.2, and 7.3. Consequently, clause 7.3 could be rephrased as follows: “*Without documented instructions from the data controller, e.g. providing for an authorisation, or a specific requirement under EU or Member State law to which the data processor is subject, the data processor cannot within the framework of the Clauses [...]*”.

2.2.7 Assistance to the data controller (Clause 8 and Appendix C.3 of the SCCs)

20. The Board is of the opinion that any reference to a specific national supervisory authority in a model contract should be avoided, since the identification of the competent supervisory authority will depend on the specific processing at stake and on the specific circumstances. Consequently, the Board recommends that the references to the Slovenian SA be removed from **clause 8.2** and be replaced, in both points a. and d., by a blank space accompanied by a note inviting the parties to specify the competent supervisory authority (e.g. “*[please indicate the competent SA]*”).

2.2.8 Notification of personal data breach (Clause 9 of the SCCs)

21. Regarding **clause 9.3** of the SCCs, the Board recommends that the reference to clause 9.2.a be replaced by a reference to clause 8.2.a. Additionally, the Board recommends that the reference to Appendix D in **clause 9.4** be replaced by a reference to Appendix C.3, and that the reference to clauses 9.1 and 9.2 in **Appendix C.3** be replaced with references to clauses 8.1 and 8.2.

22. With regard to **Appendix C.3**, the Board encourages the SI SA to avoid referring to “the role and obligations of the data processor” in the notes inviting the parties to introduce further specifications, since such broad wording might lead to uncertainty as to how the blank spaces should be filled by the parties. Consequently, the Board suggests referring to the steps to be taken by the processor and the procedure to be followed in providing assistance to the controller (with regard to data breach notifications and data protection impact assessments).

2.2.9 Erasure and return of data (Clause 10 of the SCCs and Appendix C.4)

23. Regarding **clause 10.1** of the SCCs, the Board encourages the SI SA to clarify that the processor should either delete or return the personal data (and delete copies) except for when further storage of the personal data by the processor is required by EU or Member State law. Since the exception to the legal duty refers to both Option 1 and Option 2, the words “*unless Union or Member State law requires*

storage of the personal data" should not be in bold and should be presented in a way to ensure that the parties of the contract do not understand it as only referring to the second option. The Board suggests further specifying this wording (e.g. "*unless Union or Member State law requires further storage of the personal data by the processor*").

24. In **Appendix C.4**, the Board recommends that the example should refer not only to a "time period" but also, alternatively, to an "event" ("(STATE TIME PERIOD / EVENT)") since there could be situations in which the precise time frame cannot be established but the data should be deleted after the occurrence of a specific event. Additionally, Appendix C.4 should refer to clause 10.1 instead of 11.1.

2.2.10 Audit and inspection (Clause 11 of the SCCs and Appendixes C.7 and C.8)

25. The Board recommends that the reference in **clause 11.2** to Appendixes C.6 and C.7 be replaced by a reference to Appendixes C.7 and C.8.

26. Additionally, the Board recalls that the audits referred to in Article 28(3)(h) GDPR are conducted either by the controller himself or by another auditor mandated by the controller. The Board recommends the SI SA to adapt the first scenario in **Appendixes C.7 and C.8** to specify that the third party auditor has been mandated by the controller. Consequently, the text of the examples in Appendixes C.7 and C.8 should be changed as follows: "*The data processor shall (STATE TIME PERIOD) at (THE DATA PROCESSOR'S/THE DATA CONTROLLER'S) expense **be subject to an (AUDIT/INSPECTION)** from an independent third party **mandated by the controller** concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. **The independent third party auditor will submit a (AUDITOR'S REPORT/INSPECTION REPORT).** The parties have agreed that the following types of (AUDITOR'S REPORT/INSPECTION REPORT) may be used in compliance with the Clauses: (INSERT 'APPROVED' AUDITOR'S REPORTS/INSPECTION REPORTS) [...]*".

2.2.11 Commencement and termination (Clause 13 of the SCCs)

27. Regarding **clause 13.5** of the SCCs, the Board encourages the SI SA to avoid indicating this as a specific clause as it just includes the signature of the parties and suggests that the parties and their signature should be referred to in the same way (e.g. "Name", "Position", "Date", "Signature", removing references to "Telephone number" and "Email" which will already be included in clause 14.2).

2.2.12 Data controller and data processor contacts / contact points (Clause 14 of the SCCs)

28. The Board encourages the SI SA to rephrase clause 14.1 as follows: "*Each party shall designate a person responsible for the execution of the contract*".

2.2.13 Appendix A

29. While noting that Appendix A aims at providing details about the processing activities undertaken by the data processor on behalf of the data controller, the Board recalls that the processing activities should be described by the parties in the most detailed manner possible. It is therefore important that the examples provided to illustrate the possible content of the sections of the Appendix are able to guide the parties' description.

30. In light of the above, the Board welcomes the initiative of the SI SA to include examples in **Appendix A.4** and would even suggest expanding it more, taking into account that most processing operations

involve several categories of data subjects at the same time, which in turn can be categorised in several ways, e.g. customers, consumers (adults / children), third party vendors.

2.2.14 Appendix B

31. The Board encourages the SI SA to clarify that multiple sub-processors can be listed by the parties in **Appendix B.1** although only one field has been included by way of example.

3 CONCLUSIONS

32. The Board very much welcomes the Slovenian SA's initiative to submit its draft SCCs for an opinion which aims at contributing to a harmonised implementation of the GDPR.

33. The Board is of the opinion that the draft SCCs of the Slovenian Supervisory Authority submitted for an opinion need some further adjustments in order to be considered as standard contractual clauses. If all recommendations listed in this Opinion are implemented, the SI 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.

4 FINAL REMARKS

34. This opinion is addressed to Informacijski pooblaščenec (the Slovenian Supervisory Authority) and will be made public pursuant to Article 64 (5)(b) GDPR.

35. 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 or, alternatively, the relevant grounds for which it does not intend to follow this opinion, in whole or in part. 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.

For the European Data Protection Board

The Chair

(Andrea Jelinek)