Opinion 24/2021 on the draft decision of the competent supervisory authority of Slovakia regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 20 July 2021

Table of contents

1 SUMMARY OF THE FACTS 4

2 ASSESSMENT 4

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements 4

2.2 Analysis of the SK SA's accreditation requirements for Code of Conduct's monitoring bodies 5

2.2.1 GENERAL REMARKS 5

2.2.2 INDEPENDENCE 6

2.2.3 CONFLICT OF INTEREST 6

2.2.4 EXPERTISE 6

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES 7

2.2.6 TRANSPARENT COMPLAINT HANDLING 7

2.2.7 COMMUNICATION WITH THE SK SA 7

3 CONCLUSIONS / RECOMMENDATIONS 7

4 FINAL REMARKS 7

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) 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 Article 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 when a supervisory authority (hereinafter "SA") intends to approve the requirements for accreditation of a code of conduct (hereinafter "code") monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines"), using the eight requirements as outlined in the guidelines' accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term "accreditation". However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

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

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) 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 FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Slovak Supervisory Authority (hereinafter "SK SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 25 May 2021.

2. [If applicable: In compliance with article 10 (2) of the Board Rules of Procedure, 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.]

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.

4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to "encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises." (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.

6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.

7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the SK SA to take further action.

8. This opinion does not reflect upon items submitted by the SK SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the SK SA's accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:

   a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
   b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
   c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The Board notes that the information required to be submitted within the application for accreditation includes also "results of the code of conduct monitoring audit" (section 1.6.i). Coming from the premise that the monitoring body cannot perform the monitoring of compliance with a code of conduct before its accreditation the Board is not aware of how the monitoring might be audited prior to the accreditation of the monitoring body. Therefore, the Board encourages the SK SA to modify this requirement in a comprehensible way or to exclude it from the list of information required within the application for accreditation.

2.2.2 INDEPENDENCE

11. The Board recognizes the common principle that any relationship between the monitoring body and any code member is not acceptable. The Board notes that, under section 1.7.i, the SK requirements refer to "the application shall contain the written confirmation that... there exist no relationships between the monitoring body and one or several code member/s". However, the Board considers that the way this requirement is drafted can, to some extent, be understood as that the existence of the MB relationships to (any) code members is not, in general, excluded. Therefore, the Board encourages the SK SA to modify this requirement so to make clear that this requirement refers to the relationship of the monitoring body with any code member.

12. The Board recognizes that one of the biggest risks related to the monitoring body is the risk of impartiality. The Board notes that such risk may arise not only from providing services to the code members but also from a wide range of activities carried out by the monitoring body vis-à-vis code owners (especially in the situation where the monitoring body is an internal one) or other relevant bodies of the sector concerned. On the other hand, the Board recognizes that providing non-supervisory services, purely administrative or organisational assistance or support activities may not involve a conflict of interest, as stated in the section 2.1.1.f of the draft SK accreditation requirements, provided that the impartiality of the monitoring body is not compromised. In this context, the Board encourages the SK SA to provide additional clarifications and examples of situations where there is not a conflict of interest and to revise the list of the specific examples.

2.2.3 CONFLICT OF INTEREST

13. The Board is of the opinion that examples help understand draft requirements. Therefore, the Board encourages the SK SA to include some additional examples into the draft accreditation requirements or into the complementary guidance to the requirements. In particular, the Board encourages the SK SA to add examples of situations that are likely to create a conflict of interest (section 3.1.d).

2.2.4 EXPERTISE

14. The Board notes that the minimum required education and experience of the personnel with a technical profile (set out in section 4.7.a) is limited to the field of technical/computer sciences and information system security. The Board is of the opinion that the required education and experience of the personnel with a technical profile should primarily be linked to the field of the specific sector and the particular processing activities which are the subject matter of the code of conduct. Therefore, the Board encourages the SK SA to adjust the education and experience requirement for the personnel with a technical profile taking more into account the sector and the processing activities which are the subject matter of the code of conduct.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

15. The Board notes that the wording “information on the duration or expiration of the monitoring body” (section 2.1.2.f) may not be easy to understand. The “expiration of the monitoring body” is related to the monitoring body’s mandate which is set forth in the code of conduct.. Therefore, the Board encourages the SK SA to modify this requirement accordingly .

16. The Board recognizes that a monitoring body shall be able to demonstrate the procedures for assessing the eligibility of controllers and processors to sign up and apply the code of conduct. However, the Board considers the requirement to deliver the grounds for assessing this eligibility to the SK SA (section 5.1.a) too broad and encourages the SK SA to reduce this requirement to an appropriate level.

2.2.6 TRANSPARENT COMPLAINT HANDLING

17. The Board agrees that a system of corrective measures, worked out and submitted by the monitoring body within the complaint handling procedure, has to be developed, inter alia, on the basis of corrective measures defined in the code of conduct, if the code of conduct contains such definitions. However, the wording of the SK requirements in the section 6.1.a (“... The monitoring body shall have suitable corrective measures, defined in the code of conduct...”) could be misinterpreted in the sense that the monitoring body must strictly adhere to what is defined in the code of conduct and is not obliged to develop the own consistent system of corrective measures. Therefore, the Board encourages the SK SA to rephrase the relevant requirement, in order to prevent any confusion in the interpretation of the requirement.

2.2.7 COMMUNICATION WITH THE SK SA

18. In the section 7.1.e the SK SA requires that the substantial changes to the monitoring body, of which the SK SA has to be informed without undue delay, may include, inter alia, “any changes to the basis of accreditation”. The Board encourages the SK SA to clarify in its draft accreditation requirements (section 7.1.e) the notion of the “any changes to the basis of accreditation”.

3 CONCLUSIONS / RECOMMENDATIONS

19. The Board has assessed the draft accreditation requirements of the SK supervisory authority and did not identify any issues which might lead to an inconsistent application of the accreditation of monitoring bodies.

4 FINAL REMARKS

20. This Opinion is addressed to the SK supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.

21. According to Article 64 (7) and (8) GDPR, the SK SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision.

Within the same period, it shall provide the amended draft decision 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.

22. The SK SA 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)