Opinion 11/2021 on the draft decision of the competent supervisory authority of Norway regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 23 March 2021

Table of contents

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 Norwegian Supervisory Authority (hereinafter "NO 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 26 January 2021.

2 ASSESSMENT

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

2. 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.

3. 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.

4. 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.

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

6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the NO SA to take further action.

7. This opinion does not reflect upon items submitted by the NO 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 NO SA's accreditation requirements for Code of Conduct's monitoring bodies

8. 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

9. The Board is of the opinion that examples help in understanding draft requirements. Therefore, the Board encourages the NO SA to include in the draft accreditation requirements, some additional examples. In particular, the Board encourages NO SA to add:

   - example of ad hoc internal committee as an internal monitoring body (introduction);
   - examples of services to code members or to the code owner that can adversely affect its independence (section 1.1.4);
   - examples of ways of ensuring impartiality in relation to accountability during the application process (section 1.4.3).

10. In paragraph "duration of accreditation" in the introduction, the Board notes that the reference to the periodic review does not mention that the NO SA will review the compliance with the requirements

periodically. Thus, the Board encourages the NO SA to specify the possible duration of the accreditation (for example in years or for an indefinite period of time), to clarify that the requirements may be reviewed periodically and to provide transparent information on how the periodic review will work in practice and what happens after the expiry of the validity of the accreditation.

11. The Board observes that the NO SA's draft accreditation requirements sometimes refer to an obligation ("shall") and sometimes to a possibility ("should"). For the sake of clarity, the Board recommends that the NO SA avoids the use of "should" in the text of the accreditation requirements.

2.2.2 INDEPENDENCE

12. As regards the monitoring body's independence in relation to legal and decision-making procedures, the Board underlines that it should exist not only towards the code owner, but also towards the members of the code. Thus, in section 1.1.5.h, the Board encourages making a clear reference that the independence may be demonstrated also by documents providing evidence of the business, financial, contractual, or other relations between the monitoring body and not only the code owner but also the members of the code.

13. In section 1.2.2, with respect to internal monitoring bodies, the Board encourages NO SA to add a requirement to prove that a specific separated budget is allocated to such bodies by the code owner.

14. Monitoring bodies must have sufficient financial and other resources together with the necessary procedures to ensure the functioning of the code of conduct over time. That is why, with respect to section 1.2.4 of the draft requirements, the Board encourages to NO SA to add a clear indication that financial stability and resources need to be accompanied with the *necessary procedures* to ensure the functioning of the code of conduct over time.

15. In addition, the Board considers that the requirements on financial resources would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support should not adversely affect its independence (subsection 1.2.3). For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the NO SA to provide examples of how the monitoring body can provide such evidence.

16. With respect to section 1.4.1 and demonstrating accountability by the monitoring body, the Board considers that the requirements should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. In this regard, the Board notes the example provided as to how to accomplish accountability. However, the Board believes that the example could be developed in order to make a clear reference to setting out the roles and decision-making framework and reporting procedures, and setting up policies to increase awareness among the personnel about the governance structures and the procedures in place. Thus, the Board encourages the NO SA to develop the example in this sense.

2.2.3 EXPERTISE

17. With respect to section 3.3 the Board encourages the NO SA to add examples of documentation related to the expertise of the personnel in data protection, such as trainings and data protection certificates.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

18. The Board shares the view of the NO SA whereby the monitoring body must establish procedures to assess the eligibility of controllers and processors to comply with the code. At the same time, the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of the members within a clear time frame, and check the eligibility of members prior to joining the code. Therefore, the Board recommends the NO SA to reflect this in the text.

2.2.5 REVIEW MECHANISMS

19. As regards section 7.3, the Board is of the opinion that the monitoring body should be able to contribute to reviews of the code as required by the code owner and shall therefore ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members and continues to adapt to any changes in the application and interpretation of the law and new technological developments. Therefore, the Board encourages the NO SA to reflect in the text that both, changes in the application and interpretation of the law and new technological developments, need to always be taken into consideration.

2.2.6 LEGAL STATUS

20. In section 8.2, the Board encourages the NO SA to specify that capability of being held legally responsible for monitoring activities should include that fines per Article 83(4)(c) GDPR can be imposed on the monitoring body and met.

21. In section 8.5, the Board encourages the NO SA to make a clear connection between the first and the second sentence of this section.

22. With respect to section 8.6, the Board agrees with the NO SA that a natural person must demonstrate adequate resources that allow it to act as a monitoring body. The Board encourages the NO SA to to specify how in case of natural persons the necessary expertise (legal and technical) is ensured and to add a clear reference to the necessity of ensuring and documenting how the monitoring role is guaranteed over a long term and how it can deliver the code's monitoring mechanism over a suitable period of time.

2.2.7 SUBCONTRACTING

23. As regards section 9 the Board considers that the monitoring body, in addition to be the ultimate responsible for the decision-making, is also responsible for compliance when it uses subcontractors. The Board encourages the NO SA to add the reference to compliance. Moreover, the Board encourages

NO SA to include a clear requirement for subcontractors to comply with their data protection obligations.

24. In section 9.2, the Board recommends the NO SA to add a clear indication that the monitoring body shall ensure effective monitoring of the services provided by the contracting entities. Moreover, the Board underlines the need to specify requirements relating to the termination of the contract, in particular so as to ensure that the subcontractors fulfil their data protection obligations, and encourages the NO SA to add such remark. Finally, the Board encourages the NO SA to clarify the meaning of the sentence starting with "can be demonstrated".

3 CONCLUSIONS / RECOMMENDATIONS

25. The draft accreditation requirements of the Norwegian Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:

26. Regarding "general remarks" the Board recommends that the NO SA:

- avoid the use of "should" in the text of the accreditation requirements.

27. Regarding "established procedures and structures" the Board recommends that the NO SA:

- add a clear indication that the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear time frame, and check eligibility of members prior to joining the code.

28. Regarding "subcontractors" the Board recommends that the NO SA:

- add a clear indication that the monitoring body shall ensure effective monitoring of the services provided by the contracting entities.

4 FINAL REMARKS

29. This opinion is addressed to the Norwegian supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.

30. According to Article 64 (7) and (8) GDPR, the NO 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.

31. The NO 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)