Opinion 11/2023 on the draft decision of the competent supervisory authority of Sweden regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 11 July 2023

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 Swedish Supervisory Authority (hereinafter "SE 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 16 May 2023.

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 SE SA to take further action.

7. This opinion does not reflect upon items submitted by the SE 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 SE 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 observes that the SE 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 SE SA avoid the use of "should" in the text of the accreditation requirements.

10. For the sake of consistency, the Board encourages the SE SA to adjust the terminology used in the requirements to the ones used in the Guidelines, this applies in particular to the following terms:

- in section 4.9, reference should be made to ''data processing in scope of the code'' and ''complaints received or specific incidents'';
- in sections 5.7 and 5.10, reference should be made to ''corrective measures'' instead of ''measures'';
- in section 8.3, it should be referred to ''monitoring body and related governance structures''.

11. The SE SA's draft accreditation requirements state in the introduction that an internal monitoring body "could be an internal department within the code owner or an ad hoc internal committee". The Board considers that it should be made explicit that an internal monitoring body cannot be setup within a code member. Therefore, the Board recommends adding a relevant requirement.

12. The Board notes that, in the section dedicated to the duration of accreditation, the reference to review does not mention that the SE SA will review the compliance with the requirements periodically. Thus, the Board encourages the SE 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.

2.2.2 INDEPENDENCE

13. Having examined section 1.1.3, the Board acknowledges that the SE SA states that "the duration or expiration of the mandate of the monitoring body must be regulated in such a way to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely effects the independence in carrying out the monitoring activities by the Monitoring body." The Board is of the opinion that this requirement would benefit from the inclusion of additional explanation on what duration could lead to adverse effects on the independence of the monitoring body. Therefore, the Board encourages the SE SA to include a requirement that the duration of the term of the monitoring body should be indicated.

14. With regard section 1.1.5, the Board encourages the SE SA to delete the word "undue" as a monitoring body must be free not only from "undue" but from any external pressure or influence.

15. Regarding example h) under Section 1.1.4 of the SE SA's draft accreditation requirements, the Board encourages the SE SA to clarify the terms ''associations/organisation submitting the code of conduct'' by making a reference to ''other relations between the monitoring body and not only the code owner but also the members of the code''.

16. The Board considers that, in particular in the case of an internal monitoring body, the monitoring body must prove full autonomy for the management of the budget or other resources. Accordingly, the Board recommends that the SE SA replace the term ''could'' by ''must'' in section 1.2.1.

17. The Board considers that 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. This is why, with respect to section 1.2.3 of the draft requirements, the Board encourages the SE 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.

18. As regard section 1.3.3 of the SE SA's draft accreditation requirements the Board encourages the SE SA to clarify that demonstration that the monitoring body is composed of an adequate and proportionate number of personnel could be made through procedures to appoint the monitoring body personnel, the remuneration of the said personnel, as well as the duration of the personnel's mandate, contract or other formal agreement with the monitoring body. In addition, The Board encourages the SE SA to redraft the relevant part of the requirements by adding a reference to "adequate and proportionate number of sufficiently qualified personnel".

2.2.3 CONFLICT OF INTEREST

19. The Board encourages the SE SA to clarify in section 2.1 that the staff chosen by the monitoring body or other body should be ''independent of the code member''.

20. In addition, in section 2.4, the Board encourages the SE SA to clarify that not only procedures but also ''measures'' to deal with the effects of situations identified as being likely to create a conflict of interest should be provided.

2.2.4 EXPERTISE

21. The Board notes that SE SA's draft accreditation requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. Therefore, the Board encourages the SE SA to clarify in section 3 which requirement should be met by the staff performing the monitoring function and the personnel making the decisions.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

22. Furthermore, the Board considers that the examples in section 4.3 could be further substantiated, in accordance with paragraph 72 of the Guidelines, by referring to the different ways in which such investigations can be conducted, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. Therefore, the Board encourages the SE SA to redraft the requirement, to make clear that the audit can be carried out in different ways.

23. Moreover, the Board notes that section 4.4 refers to the obligation for monitoring bodies to establish ad hoc procedures to actively and effectively monitor the code members' compliance with the code's provisions. In order to ensure consistency with the wording used in section 4.2 the Board encourages the SE SA to amend the wording to refer to ''upfront, ad hoc and regular procedures''.

2.2.6 TRANSPARENT COMPLAINT HANDLING

24. According to section 5.10, the monitoring body *could* make information concerning any sanctions leading to suspension or exclusion of code members – and any subsequent lifting hereof – publicly available. Without prejudice to national legislation, the Board encourages the SE SA to replace the term ''could'' by ''must'' and to amend this requirement to provide that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate.

25. The Board notes that section 5.7 of the SE SA's draft accreditation requirements refers to the obligation for monitoring bodies to inform the SA of the measures taken and the reasons for taking them. In line with paragraph 77 of the Guidelines, the Board recommends that the SE SA amend this requirement in order to clarify that this notification should also be made to ''the competent SA and, where required, all concerned SAs''.

2.2.7 COMMUNICATION WITH THE SE SA

26. With regard to section 6 of the SE SA's draft accreditation requirements, the Board recommends that the SE SA make reference to the effective communication with other competent supervisory authorities and not only with the SE SA, as far as transnational codes are concerned.

27. The Board understands that section 6.2 of the requirements refers to the information that the monitoring body will provide to the SE SA upon request. The Board is of the opinion that the requirement to communicate ''any actions'' need to address such areas as: actions taken in cases of infringement of the code and the reasons for taking them (article 41 (4) GDPR), periodic reports, reviews or audit findings. Therefore, the Board encourages the SE SA to clarify this requirement accordingly.

2.2.8 REVIEW MECHANISMS

28. 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 SE SA to reflect in the text that both changes in the application and interpretation of the law and/or new technological developments need to always be taken into consideration.

2.2.9 LEGAL STATUS

29. In section 8.2, the Board encourages the SE 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.

30. In section 8.5, the Board encourages the SE SA to make a clear connection between the first and the second sentence of this section. In addition, the Board encourages the SE SA to clarify that, in order to demonstrate the continuity of the monitoring function, the monitoring body should demonstrate that it has sufficient financial and other resources, and the necessary procedures.

31. With respect to section 8.6, the Board agrees with the SE SA that a natural person must demonstrate adequate resources that allow it to act as a monitoring body. The Board encourages the SE SA 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.

2.2.10 SUBCONTRACTING

32. As regards section 9 of the SE SA's draft accreditation requirements, the Board encourages the SE SA to add the reference to compliance. Moreover, the Board encourages the SE SA to include a clear requirement for subcontractors to comply with their data protection obligations.

33. In section 9.2, the Board recommends that the SE SA 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 SE SA to add such requirement.

3 CONCLUSIONS / RECOMMENDATIONS

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

35. Regarding *general remarks* the Board recommends that the SE SA:

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

    2. make explicit that an internal monitoring body cannot be setup within a code member.

36. Regarding *independence* the Board recommends that the SE SA:

    1. replace the term ''could'' by ''must'' in section 1.2.1.

37. Regarding *transparent complaint handling* the Board recommends that the SE SA:

1. amend section 5.7 in order to clarify that this notification should also be made to ''the competent SA and, where required, all concerned SAs''

38. Regarding *communication with the SE SA* the Board recommends that the SE SA:

1. make reference in section 6 to the effective communication with other competent supervisory authorities and not only with the SE SA, as far as transnational codes are concerned

39. Regarding *subcontracting* the Board recommends that the SE SA:

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

4 FINAL REMARKS

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

41. According to Article 64 (7) and (8) GDPR, the SE 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.

42. The SE 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

(Anu Talus)