

Opinion of the Board (Art. 64)



Opinion 18/2020 on the draft decision of the competent supervisory authority of the Netherlands regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 23 July 2020

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 NL 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	EXPERTISE	7
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES	8
2.2.5	TRANSPARENT COMPLAINT HANDLING	8
2.2.6	CONFLICT OF INTEREST	9
2.2.7	REVIEW MECHANISMS	9
2.2.8	LEGAL STATUS	10
3	CONCLUSIONS / RECOMMENDATIONS	10
4	FINAL REMARKS.....	11

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 Dutch Supervisory Authority (hereinafter "NL 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 28 May 2020.

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 NL SA to take further action.
7. This opinion does not reflect upon items submitted by the NL 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 NL 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, according to the general notes of the draft accreditation requirements, the NL SA reserves the right to conduct a risk-based review of the monitoring body to ensure that the body still meets the requirements for accreditation, whereas such a review could be initiated by (but is not limited to): amendments to the code of conduct, substantial changes to the monitoring body or the monitoring body failing to deliver its monitoring functions. The Board welcomes the provision concerning the re-assessment, according to a risk-based approach, of the accreditation requirements by the NL SA in order to ensure compliance with the GDPR. However, for the sake of clarity and transparency, the Board recommends the NL SA to explicitly state that in case of substantial changes to the monitoring body relating to the monitoring body’s ability to function independently and effectively, such a review will be always conducted.
10. The Board encourages the NL SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.

2.2.2 INDEPENDENCE

11. The Board observes that the NL SA's 'explanatory notes' section concerning the requirements for independence, refer to independence "*from the code owner or the code members*". As stated in the Guidelines, the independence of the body concerned should be demonstrated in relation also to the profession, industry or sector to which the code applies (para. 63). Therefore, the Board recommends that the NL SA redraft this reference in line with the Guidelines and put it in the 'requirements' section – so as to clarify that this is a requirement itself.
12. The Board notes that the first paragraph of section 1.1 in the NL SA's draft accreditation requirements fits better into the relevant 'explanatory notes' section. Therefore, the Board encourages the NL SA to appropriately move this paragraph.
13. The Board welcomes the requirement that the legal structure of the monitoring body, including its ownership, must shield the monitoring body from external influence (subsection 1.1.1 in the NL SA's draft accreditation requirements), as well as the provision of relevant examples of how this might be demonstrated. However, the Board encourages the NL SA to clarify that this external influence should be considered with respect to the code owner and the code members. Moreover, with regard to the relevant examples, the Board encourages the NL SA to clarify the term 'articles of incorporation', as well as to add, as a relevant example, that the duration, or expiration of the mandate of the monitoring body should be fixed in such a way as to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely affects the independence in carrying out the monitoring activities by the monitoring body.
14. Furthermore, the Board is of the opinion that internal monitoring bodies can be set up only within a code owner. Therefore, the Board recommends that this is clarified and reflected in the text of the draft accreditation requirements in the subsection 1.1.2 – e.g. by replacing "for example" with "in particular".
15. In subsection 1.1.3 in the NL SA's draft accreditation requirements, it is stated that "*the monitoring body shall demonstrate organisational independence, for example, an internal monitoring body may use different logos or names where appropriate*". The Board welcomes such an example; however, especially for the case of internal monitoring bodies, the Board encourages the NL SA to add more concrete examples of evidence illustrating organizational independence of an internal monitoring body, such as, e.g., information barriers and separate reporting structures.
16. With regard to the legal status and decision-making process (section 1.1 in the NL SA's draft accreditation requirements), the Board acknowledges the impartiality of the monitoring body from the code members. However, the Board is of the opinion that these requirements should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members, as well as with regard to the profession, industry or sector to which the code applies. For this reason, the Board encourages the NL SA to amend this section accordingly.
17. Furthermore, the Board considers that the section concerning the financial independence (section 1.2 in the NL SA's draft accreditation requirements) should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. These include the number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the

processing operation(s). Therefore, the Board encourages the NL SA to redraft the requirements accordingly.

18. Moreover, as for the financial requirements (section 1.2), the Board considers that such requirements 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 1.2.2). 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 NL SA to provide examples of how the monitoring body can provide such evidence.
19. The Board welcomes the provision in the subsection 1.3.1 in the NL SA's draft accreditation requirements that *"the monitoring body shall demonstrate that it has adequate resources and personnel to effectively perform its tasks"*. The Guidelines though provide further specialisation on this, stating that the resources should be proportionate to the expected number and seize of code members, as well as the complexity or degree of risk of the relevant data processing. Therefore, the Board encourages the NL SA to redraft this requirement in line with the Guidelines.
20. Moreover, with respect to subsection 1.3.1, the Board encourages the NL SA to include a reference to technical resources necessary for the effective performance of the monitoring body's tasks.
21. Subsection 1.3.3 (under the section on "organisational independence") refers to the use of sub-contractors by the monitoring body. The Board is of the opinion that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. Although the Board identifies that the examples given in this subsection are in this direction, the Board recommends the NL SA to explicitly clarify this requirement in the draft accreditation requirements.
22. The Board observes that, according to subsection 1.3.3 of the NL SA's draft accreditation requirements, when using sub-contractors for processes relating to monitoring actions, evidence for demonstrating that the use of subcontractors does not remove or diminish the responsibility of the monitoring body may include *"written contacts or agreements to outline for example responsibilities, confidentiality, what type of data will be held and a requirement that the data is kept secure"*, as well as a documented clear procedure for subcontracting. The Board encourages the NL SA to redraft the text in order to include requirements relating to the termination of those contracts, in particular so as to ensure that the subcontractors fulfil their data protection obligations.
23. The Board observes that subsection 1.4.1 under the section on "accountability" is more related to legal and decision making procedures (i.e. to section 1.1) than accountability. Therefore, the Board encourages the NL SA to make an appropriate amendment in the text.

2.2.3 EXPERTISE

24. Regarding the accreditation requirement in terms of the expertise of the monitoring body (section 2 in the NL SA's draft accreditation requirements), the Board acknowledges that the guidelines set a high bar requiring monitoring bodies to have an in-depth understanding of data protection issues.

Therefore, the Board encourages the NL SA to appropriately amend the relevant requirement in the subsection 2.2.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

25. The Board observes the NL SA's draft accreditation requirements refers twice to "the number of code members". More precisely, in the third paragraph in the 'explanatory notes' subsection of section 3 on established procedures and structures, the number of code members is being mentioned as a factor to be taken into account by the monitoring procedures. The Board also notes the same reference to 'number of code members' in requirements 3.2. Provided that the number of code members might not be known when the monitoring body applies for accreditation and that may change considerably after the accreditation has been granted, the Board recommends the NL SA to include, in both above places, appropriate references to "the expected number and size of code members", to align the text with the Guidelines and allow for more flexibility.
26. Moreover, in the same subsection, it is stated (last paragraph) that "*the monitoring body shall apply the penalties as defined in the code of conduct*". By only referring to penalties, the explanatory note seems to restrict the margin of manoeuvre of the monitoring body with regard to the kind of measures it can apply. The Board considers that a more comprehensive wording would also mention corrective measures, and encourages the NL SA to add the suggested reference in the explanatory note.
27. With regard to established procedures and structures (section 3 in the NL SA's draft accreditation requirements), the Board is of the opinion that the procedures to monitor compliance with codes of conduct have to be specific enough to ensure a consistent application of the obligations of code monitoring bodies. In particular, the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear timeframe, and check the eligibility of members prior to joining the code. Therefore, the Board recommends that the NL SA develop further these requirements and add examples of the above procedures (such as, procedures providing for audit plans to be carried out over a definite period and on the basis of predetermined criteria).

2.2.5 TRANSPARENT COMPLAINT HANDLING

28. With regard to the complaints handling procedure, the Board observes that the explanatory note (section 4 in the NL SA's draft accreditation requirements) states that "*personnel will demonstrate sufficient knowledge and impartiality*". The Board considers that the level of knowledge required to handle complaints would be better understood if the NL SA refers to "adequate knowledge" defining its meaning and therefore it encourages the NL SA to do so.
29. The Board notes that in the subsection 4.1 in the NL SA's draft accreditation requirements regarding complaints against code members, it is stated that "*the monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling and decision-making process*". The Board encourages the NL SA to consider practical examples for the process of a complaints handling procedure, such as that the monitoring body should outline a procedure to receive, manage and process complaints, which in turn shall be publicly available and easily accessible.
30. The Board observes that in the subsection 4.4 in the NL SA's draft accreditation requirements it is stated that the monitoring body should inform the SA about the measures taken and justification of

any infringements leading to code member suspension or exclusion. However the Board recommends the NL SA to also include the notification to the code members and code owner as explicit requirements, in line with the Guidelines.

31. Regarding section 4.6 in the NL SA's draft accreditation requirements, the Board notes that the decisions of the monitoring body shall be made publicly available in line with its complaints handling procedure, whereas this information could include but is not limited to, general statistical information concerning the number and type of complaints/infringements and the resolutions/corrective measures issued and shall include information concerning any sanctions leading to suspensions or exclusions of code members. Without prejudice to national legislation, the Board encourages the NL SA to amend this requirement so 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.

2.2.6 CONFLICT OF INTEREST

32. The Board takes note that in the NL SA's 'explanatory notes' section concerning the requirements for non-conflict of interest, some possible sources of risks to impartiality of the monitoring body are being described. However, the Board is of the opinion that, for practical reasons, more concrete examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for any of the organisations adhering to the code. In order to avoid any conflict of interest, the personnel would declare their interest and the work would be reallocated. Therefore, the Board encourages the NL SA to add some examples in the requirements.
33. The Board notes that in the Section 5.1 in the NL SA's draft accreditation requirements, it is stated that *"the monitoring body shall have in place a documented procedure to identify, analyse, evaluate, treat, monitor and document on an ongoing basis any risks to impartiality arising from its activities"*. The Board recommends the NL SA, in line with the Guidelines, to amend this requirement so as to explicitly stress that the monitoring body shall refrain from any action incompatible with its tasks and duties.
34. The Board also notes that the monitoring body, according to the subsection 5.2 in the NL SA's draft accreditation requirements, shall choose or direct and manage its personnel. The Board is of the opinion that this requirement should be aligned with the Guidelines by explicitly adding the possibility that the staff can be provided by other body independent of the code. In this direction, some examples might also be helpful. An example of staff provided by a body independent of the code would be monitoring body personnel that have been recruited by an independent external company, which provides recruitment and human resources services. Therefore, the Board encourages the NL SA to appropriately amend this requirement.

2.2.7 REVIEW MECHANISMS

35. The Board observes that, in the subsection 7.1 in the NL SA's draft accreditation requirements, it is stated that *"the monitoring body will 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 meet the application of the GDPR"*. In line with the Guidelines, the review mechanisms should take into account any changes in the application and interpretation of the law or where there are new technological developments

which have impact upon the data processing carried out by the code members or the provisions of the code. Therefore, the Board encourages the NL SA to appropriately enrich this requirement.

2.2.8 LEGAL STATUS

36. With regard to the legal status of the monitoring body, the NL SA's explanatory note for this section states that the monitoring body "*must demonstrate sufficient financial and other resources to deliver its specific duties and responsibilities*". The Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. Thereby, the Board encourages that the NL SA amend the explanatory note, adding the above-mentioned reference to "procedures".
37. Moreover, the code of conduct itself will need to demonstrate that the operation of the code's monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that a monitoring body demonstrates that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. Therefore, the Board recommends NL SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.

3 CONCLUSIONS / RECOMMENDATIONS

38. The draft accreditation requirements of the NL Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
39. Regarding *general remarks* the Board recommends that the NL SA:
 1. Explicitly state that in case of substantial changes to the monitoring body relating to the monitoring body's ability to function independently and effectively, a review of the body to ensure that it still meets the requirements for accreditation will be always conducted.
40. Regarding *independence* the Board recommends that the NL SA:
 1. Redraft the explanatory note reference to 'requirements for independence' so that it is in line with the Guidelines, pointing out that the independence should be demonstrated in relation also to the profession, industry or sector to which the code applied, and put in the 'requirements' section;
 2. Clarify in the paragraph 1.1.2 that internal monitoring bodies can be set up only within a code owner.
 3. Add in section 1.3.3 that when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.
41. Regarding *conflict of interest* the Board recommends that the NL SA:
 1. To amend the requirement in Section 5.1 so as to explicitly stress that the monitoring body shall refrain from any action incompatible with its tasks and duties, in line with the Guidelines.
42. Regarding *established procedures and structures* the Board recommends that the NL SA:

1. Include appropriate references to “the expected number and size of code of code members” in the ‘explanatory notes’ subsection of section 3 and in the requirements 3.2, to align the text with the Guidelines and allow for more flexibility.

2. Further develop under section 3 the procedures to monitor compliance with codes of conduct and includes examples of such procedures.

43. Regarding *transparent complaint handling* the Board recommends that the NL SA:

1. Include in the requirements 4.4 that information about the measures taken and justification of any infringements leading to code member suspension or exclusion should be additionally provided to the code members and code owner, in line with the Guidelines.

44. Regarding *legal status* the Board recommends that the NL SA:

1. Require that the monitoring body should demonstrate that it can deliver the code’s monitoring mechanism over a suitable period of time.

4 FINAL REMARKS

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

46. According to Article 64 (7) and (8) GDPR, the NL 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.

47. The NL 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) (γ) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)