

Opinion of the Board (Art. 64)



Opinion 31/2020 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 07 December 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 PL SA’s accreditation requirements for Code of Conduct’s monitoring bodies5
 - 2.2.1 GENERAL REMARKS 5
 - 2.2.2 INDEPENDENCE 6
 - 2.2.3 CONFLICT OF INTEREST 8
 - 2.2.4 EXPERTISE 8
 - 2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES 9
 - 2.2.6 TRANSPARENT COMPLAINT HANDLING 9
 - 2.2.7 COMMUNICATION WITH THE PL SA..... 9
 - 2.2.8 REVIEW MECHANISMS 10
 - 2.2.9 LEGAL STATUS 10
- 3 CONCLUSIONS / RECOMMENDATIONS 11
- 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 Polish Supervisory Authority (hereinafter "PL 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 9 October 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 PL SA to take further action.
7. This opinion does not reflect upon items submitted by the PL 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 PL 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 would like to underline that the obligation of the monitoring body to demonstrate compliance with the accreditation requirements is not limited to the moment it applies for accreditation, but it is an ongoing obligation. In other words, the monitoring body should be able to demonstrate compliance with the requirements at all times.
10. With regard to § 1, section 6.3 of the PL SA’s draft accreditation requirements, the Board notes that the reference to the periodic review does not mention that the SA will review the compliance with the requirements periodically. Thus, the Board encourages the PL SA 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 notes that the requirements include a section on definitions. In this respect, the Board encourages the PL SA to use consistency wording when referring to monitoring body personnel, in

order to avoid confusion. Thus, references to “staff” should be avoided and the correct term should be used when referring to the monitoring body personnel. The Board encourages the PL SA to make the necessary changes (e.g. in sections 2.2, 2.6 under § 3) in order to refer to the monitoring body personnel in a consistent manner.

12. In addition, the Board encourages the PL SA to revise the requirements in order to avoid misunderstandings stemming from the translation of the document into English (for example, “accreditation criteria” should be replaced by “accreditation requirements”; section 4.1.3.3 under § 3 should refer to audit of the member/candidate, instead of “from”; last sentence of section 5.11 under § 3 should read “for example by asking him to confirm it”, instead of “to do so”; the reference under section 5.12 under § 3 to “an amicable settlement procedure established by it” should be replaced by “[...] established by the monitoring body”; the reference to the monitoring body’s “seat” in section 8.1 under § 3 should be replaced by “establishment” and the reference to the “sharing of responsibility” in section 8.3 under § 3 should be replaced by “bearing of responsibility”, as the Board understands it is a translation mistake).

2.2.2 INDEPENDENCE

13. With regard to the specific requirements for accreditation of the monitoring body (under § 3 of the PL SA’s draft accreditation requirements), the Board considers that the requirements to demonstrate the independence of the monitoring body (section 1 under § 3) would benefit from the inclusion of examples with regard to the four areas where independence has to be demonstrated. For example, organisational independence can be demonstrated with a differentiated payroll, analytical accounting systems with different responsibility centres or any other logical separation that can rise firewalls between the monitoring body and the code owners or code members. As for financial independence, 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 PL SA to provide examples of how the monitoring body can provide such evidence
14. With respect to definition of independence, the Board encourages the PL SA to elaborate what independence means. To ensure consistency such clarification could rely on the wording agreed by the Board in the previous opinions. According to the Board, independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. In Board’s view these rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, nor subject to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself.
15. The Board observes that the draft accreditation requirements do not make an explicit reference to “accountability” as one of the four areas in which the monitoring body shall demonstrate independence. The Board considers that the independence of the monitoring body shall be demonstrated in four areas: 1) Legal and decision making procedures, 2) financial, 3) organisational

and 4) accountability.² Therefore, the Board recommends that the PL SA to include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.

16. With regard to the first paragraph of section 1 under § 3 of the PL SA's draft accreditation requirements ("Independence"), the Board considers that the impartiality of the monitoring body from the code members, the profession, industry or sector to which the code applies 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. In addition, the impartiality must be demonstrated also in relation to the profession or sector. For this reason, the Board encourages the PL SA to amend this paragraph accordingly. In addition, the Board considers that other references to the industry (for example, in sections 3 and 7 under § 3), should be completed in the same line, in order to avoid confusion.
17. With regard to internal monitoring bodies, subsection 1.1.2 under § 3 of the PL SA's draft accreditation requirements refer to the independence of the internal monitoring body in relation to the code owner. The Board recognised the importance of ensuring the impartiality of internal monitoring bodies from the code owner. However, the independence shall also be ensured with regard to code members. Thus, the Board recommends the PL SA to include a reference to the code members as well.
18. With regard to section 1.2 under § 3, the Board considers that the requirements concerning the financial independence 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 PL SA to redraft the requirements accordingly.
19. With regard to the example given on subsection 1.2.1 under § 3 as to the source of funding, the Board underlines that in any case, the independence of the monitoring body cannot be in any way compromised. For instance, the monitoring body would not be considered to be 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 PL SA to add such clarification and examples. In addition, the Board notes that subsection 1.2.1 under § 3 refers to the fees and contributions paid by the code members' candidates. The Board encourages the PL SA to clarify the reference to the code members' candidates.
20. With regard to subsection 1.2.3 under § 3 of the PL SA's draft accreditation requirements, the Board understands that it refers to the long-term financial stability of the monitoring body. However, the Board considers it could be better clarified, to ensure that the monitoring body has procedures in place to ensure its long-term financial stability and that the loss of one or more funding sources does not affect independence. Therefore, the Board encourages the PL SA to include such clarification.
21. With regard to the organisational independence (section 1.3 and in particular, subsection 1.3.2 under § 3), the Board encourages the PL SA to clarify that "material resources" also include technical resources.

² The EDPB developed these areas in more detail in the Opinion 9/2019 on the Austrian SA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

22. Regarding subsection 1.3.4 under § 3, the Board notes that the allocation of resources will depend, inter alia, on the “number of code members”. Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the PL SA to refer to the expected number and size of the code members.
23. With regard to subsection 1.3.6 under § 3, the Board notes that the obligation of the monitoring body to demonstrate independence is only “during the decision-making process”. The Board considers that the independence of the monitoring body is an ongoing process and must be ensured and demonstrated at any time, not only during the decision-making process. In addition, the Board underlines that, in order to demonstrate organisational independence, the monitoring body personnel shall be able to act independently from the code owner and the code members and without being subject to any pressure or influence. Finally, the Board welcomes the inclusion of the example in subsection 1.3.6 under § 3. However, in order to avoid confusion, the example should clearly indicate that it is related to the selection procedure and that the independence of the monitoring body personnel is not limited to the selection procedure, as reflected in the examples provided in par. 13 of this Opinion. Therefore, the Board recommends the PL SA to amend the draft requirements in order to reflect the abovementioned changes.

2.2.3 CONFLICT OF INTEREST

24. As a general remark in this section, the Board is of the opinion that, for practical reasons, 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 the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the PL SA to add some examples, similar to the one provided in this paragraph.
25. Furthermore, the Board observes that the PL SA’s draft accreditation requirements do not explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties and to not seek nor take instructions from any person, organisation or association (paragraph 68, page 23 of the Guidelines). Therefore, the Board recommends the PL SA to align the text with the Guidelines by including the above-mentioned obligations.

2.2.4 EXPERTISE

26. Regarding the accreditation requirement in terms of the expertise of the monitoring body (section 3 of the PL 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. In addition, the guidelines also require an expert knowledge of the specific processing activities which are the subject matter of the code. The Board acknowledges that section 3.3 under § 3 of the PL SA’s draft accreditation requirements address the level of expertise and encourages the PL SA to amend it in order to align the requirements with the guidelines.
27. With regard to section 3.1 under § 3 of the PL SA’s draft accreditation requirements, the Board notes that the requirement implies that specific expertise requirements will be laid down in the Code. Whereas the Board welcomes the drafting of codes that include specific expertise requirements, it is also aware that it may not always be the case. Thus, in order to reflect that, the Board encourages the PL SA to replace “will” by “may”.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

28. With regard to subsection 4.1.3.2 under § 3, the Board notes that the audit methodology will take into account the “number of code members”. Since the number of code members may not be known at the moment the monitoring body applies for accreditation, the Board encourages the PL SA to refer to the expected number and size of the code members and the complaints received.

2.2.6 TRANSPARENT COMPLAINT HANDLING

29. Regarding subsection 5.4.3 under § 3 of the PL SA’s draft accreditation requirements, the Board acknowledges that the complaints handling procedure shall include, at least, “time limits for dealing with the complaint”. The Board is of the opinion that further clarification is needed with regard to the time limits for dealing with complaints. In this regard, the procedure should envisage that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame (e.g. 3 months). This period could be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation. Therefore, the Board recommends that the PL SA redraft the requirement accordingly.
30. With regard to section 5.7 under § 3 of the PL SA’s draft accreditation requirements, the Board encourages the PL SA to redraft it as an actual requirements (i.e. starting with “the monitoring body shall...”).
31. Section 5.8 under § 3 of the PL SA’s draft accreditation requirements establishes the obligation of the monitoring body to inform the SA “of the actions taken in respect of complaints submitted”. The Board notes that the information obligation is also towards the code member, the code owner and all concerned SAs, as stated in the Guidelines (par. 77). Therefore, the Board recommends that the PL SA amend the requirement accordingly.

2.2.7 COMMUNICATION WITH THE PL SA

32. Section 6.1 under § 3 of the PL SA’s draft accreditation requirements establishes the obligation of the monitoring body to submit an annual report to the SA on all its activities in relation to the Code of Conduct. The following sections also develop situations in which the monitoring body will communicate with the PL SA. In addition, subsection 4.1.3.8 establishes regular reporting obligations of the monitoring body. The Board considers that the information on the functioning of the monitoring body activities (for example, actions taken by the MB) should also be available to the PL SA on its request, and encourages the PL SA to include such reference.
33. In addition, the Board encourages the PL SA to make the link between subsection 6.2.6 under § 3 and subsection 6.2.8 under § 3 clearer, in order to avoid misunderstandings with regard to the type of audits.
34. Regarding section 6.3 under § 3, the Board notes that the example given would only be relevant in case the code of conduct covers the obligations under article 33 GDPR. Therefore, the Board encourages the PL SA to clarify this in the example.
35. Regarding section 6.5 under § 3, the Board notes that the accreditation requirements state that significant changes “may result in a review of the accreditation”. The Board is of the opinion that, when a substantial change has been performed, the review of the accreditation is not merely a possibility, but rather an obligation. Therefore, the Board recommends the PL SA to rephrase the wording, by stating that substantial changes would result in a review of the accreditation.

2.2.8 REVIEW MECHANISMS

36. Section 7.1 under § 3 of the PL SA's draft accreditation requirements establishes the obligation of the monitoring body to provide a procedure to assist with the periodic review of the code of conduct. The Board is of the opinion that the monitoring body also has a key role in applying code updates (amendments of extensions of the code) following the instructions of the code owner, and encourages the PL SA to include such reference. In addition, the Board considers that the reference to section 4.1.3 under § 3 should be replaced by 4.1.4 under § 3 and that a reference to section 6.2.5 under § 3 would be helpful, as an example of the elements to be considered, and encourages the PL SA to amend the draft accordingly.
37. With regard to section 7.5 under § 3, the Board notes the reporting is only to the code owner. The Board encourages accreditation requirements which require a monitoring body to develop mechanisms that enable feedback to the code owners and to any other entity referred to in the code of conduct. Therefore, the Board encourages the PL SA to include the abovementioned reference in the draft requirements.
38. In addition, the Board considers that the information related to the review carried out should be at the disposal of the SA, and encourages the PL SA to amend the draft accordingly.

2.2.9 LEGAL STATUS

39. With regard to section 8.3 under § 3, the Board underlines that the monitoring body should have financial and other resources, and the necessary procedures to ensure the monitoring body activity. Thereby, the Board encourages that the PL SA specify that the monitoring body shall have adequate financial and other resources and the necessary procedures to ensure its functioning.
40. 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 PL SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.
41. The Board observes that, according to subsection 8.7.1 under § 3 of the PL SA's draft accreditation requirements, when using sub-contractors for processes relating to monitoring actions, evidence for demonstrating the compliance of the subcontractor with the requirements may include "a contract setting out the responsibilities and responsibilities of the parties, confidentiality, the categories of personal data processed and the obligation to provide adequate security for them". The Board encourages the PL 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.
42. The Board notes that section 8.9 under § 3 states that "the use of subcontracting does not exempt the monitoring body from the responsibility of the monitoring body under the GDPR". 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 realises that section 8.9 under § 3 seems to imply that, the Board recommends the PL SA to explicitly clarify it. In addition, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the PL SA to specify that, notwithstanding the

sub-contractor's responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance.

3 CONCLUSIONS / RECOMMENDATIONS

43. The draft accreditation requirements of the Polish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
44. Regarding *independence* the Board recommends that the PL SA:
 1. include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.
 2. include a reference to code members with regard to the independence of internal monitoring bodies in subsection 1.1.2 under § 3.
 3. amend subsection 1.3.6 under § 3 in order to reflect the remarks made in paragraph 23 of this Opinion
45. Regarding *conflict of interest* the Board recommends that the PL SA:
 1. explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties and to not seek nor take instructions from any person, organisation or association
46. Regarding *transparent complaint handling* the Board recommends that the PL SA:
 1. redraft subsection 5.4.3 under § 3 in order to take into account that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame (e.g. 3 months). This period could be extended when necessary.
 2. include, among the addressees of the information referred to in section 5.8 under § 3, the code member, the code owner and all concerned SAs.
47. Regarding *communication with the PL SA* the Board recommends that the PL SA:
 1. rephrase the wording in section 6.5 under § 3, by stating that substantial changes would result in a review of the accreditation.
48. Regarding *legal status* the Board recommends that the PL SA:
 1. amend the requirements in order to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.
 2. clarify, section 8.9 under § 3, that even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity

4 FINAL REMARKS

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

50. According to Article 64 (7) and (8) GDPR, the PL 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.
51. The PL 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)