
# Opinion 20/2020 on the draft decision of the competent supervisory authority of Greece 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 EL SA's accreditation requirements for Code of Conduct's monitoring bodies 5

2.2.1 GENERAL REMARKS ..... 5

2.2.2 INDEPENDENCE ..... 7

2.2.3 CONFLICT OF INTEREST ..... 8

2.2.4 EXPERTISE ..... 9

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES ..... 9

2.2.6 TRANSPARENT COMPLAINT HANDLING ..... 9

2.2.7 REVIEW MECHANISMS ..... 10

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 Hellenic Supervisory Authority (hereinafter "EL 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. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

# 2 ASSESSMENT

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

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

4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

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

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

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

8. This opinion does not reflect upon items submitted by the EL 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 EL SA's accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:

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

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

10. The Board is of the opinion that examples help in understanding draft requirements. Therefore, the Board encourages the EL SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some additional examples. In particular, the Board encourages EL SA to add:

- examples of the information or documents that applicants have to submit when applying for accreditation;
- examples of what may constitute an internal monitoring bodies (i.e. ad hoc internal committee or separate department within the organisation of the code owner; section 1 of the draft requirements);

- examples of data protection expertise (e.g. expertise may be demonstrated for example by submitting evidence of adequately trained educated and experienced staff in these domains, for example by means of a diploma, certification or a proof of experience; section 3 of the draft requirements);
- examples of significant changes taking place in the body which lead to the need for reaccreditation (e.g. any change that impacts on the monitoring body's ability to perform its function independently and effectively or would be likely to call into question its independence, expertise and the absence of any conflict of interests or to adversely affect its full operation);
- examples of the kind of information that the monitoring body is expected to include in the annual report (section 7a of the draft requirements);
- examples of the different ways a monitoring body can be set up (i.e. a limited company, an association, an internal department within the code owner's organisation or as a natural person; section 8 of the draft requirements).

11. According to the Guidelines, codes are a mechanism which can be used to assist organisations in demonstrating their compliance with the GDPR (paragraph 10 of the Guidelines). In this context, it should be noted that specific rules and/or practices cannot ensure compliance with the overall conditions for lawful processing of personal data as set out in the GDPR. Therefore, the Board recommends to the EL to replace in the second paragraph of the introduction the phrase "ensure compliance" with "help ensuring compliance" or "assist organisations in demonstrating compliance".

12. In the third paragraph of the introduction, the Board encourages EL SA to include a reference to Art. 40.5 of the Regulation, this would allow to keep consistency with other paragraphs where references to relevant provisions of the GDPR are included. Also, in the Board's opinion an approved code of conduct can be used not as an evidence, but only as supporting evidence to demonstrate compliance with the obligations of the controller/ processor - the Board encourages EL SA to introduce relevant changes.

13. In paragraph nine of the introduction, the Board encourages EL SA to use the term "monitoring body" instead of body. Also phrase "associated with" shall be replaced with a sentence that the accreditation of a monitoring body applies only for a specific code, as indicated in the Guidelines (see definition of the accreditation).

14. As regards paragraph 10 of the draft requirements, the Board would like to underline that the accreditation requirements may be reassessed sooner than after 5 years. Therefore the Board encourages EL SA to clarify that the requirements may be reviewed periodically, also before the end of the 5 years period. Moreover, the Board notes that it is only the monitoring body that it allowed to submit a request for renewal to the supervisory authority. Therefore, the Board recommends to remove a reference to the code owner, when mentioning request for renewal in this paragraph.

15. In relation to the codes that are used as instruments for international transfers (paragraph 11 of the introduction), the Board recommends EL SA to delete the last part of the last sentence, i.e. "which will be considered in separate guidelines", as it refers to a future event.

16. With respect to basic definitions and the definition of a "code member" the Board encourages EL SA to remove a reference to adherence. If a controller or processor signed up to the code it also means that he adhered to the code and its obligations.

17. Finally, the Board encourages EL SA to ensure consistency in wording used, in particular regarding references to EL SA (HDPA and Authority are used interchangeably).

### 2.2.2 INDEPENDENCE

18. With respect to definition of independence, the Board encourages EL 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.[2]

19. In Board's view, when the monitoring body is part of the code owner organisation, particular focus must be made on their ability to act independently. Rules and procedures have to be established to ensure that this committee acts autonomously and without any pressure from the code owner or the code members. Bearing the above in mind, with respect to organisational independence, the Board recommends EL SA to elaborate and better explain in the section 1 of the draft requirements what is the ability of a monitoring body to act independently.

20. The Board encourages, for the sake of consistency with previous opinions, to replace the headline "Legal independence in decision-making procedures" with "Legal and decision making procedures".

21. In section 1.i.A, the Board, taking into consideration the importance of the ability to act independently, encourages EL SA to replace "independent in making decisions" with a more broad term "independent in decision making procedures".

22. For the sake of consistency with previous opinions, in section 1.i.B the Board encourages EL SA to replace references to "people" with "personnel". Also, the Board encourages EL SA to be consistent in use of "shall/should/must". With respect to ensuring that the monitoring body shall neither receive nor take instructions/guidance from anyone, EL SA is encouraged to indicate that this requirement applies not only to the monitoring body but also to its personnel involved in decision-making process. As regards the example provided by EL SA and the reference to documents and recorded procedures currently applicable establishing its independence in decision making, the Board recommends deletion of the word "current" - in the opinion of the Board such documents and recorded procedures must be in place all the time.

23. As regards section 1.i.C and the internal monitoring body, the Board notes that the requirement that an internal monitoring body cannot be setup within a code member seems to be missing. Therefore, the Board recommends adding a relevant provision.

[2] See paragraph 14 of Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR.

24. The monitoring body 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.ii.A of the draft requirements, the Board recommends to clarify that long-term financing should be ensured.

25. With respect to section 1.iii.A, the Board encourages EL SA to explain what does "necessary" human resources mean. The Board encourages EL SA to consider making a reference to "sufficient numbers of sufficiently qualified personnel". Also, the Board encourages EL SA to include a reference to technical resources necessary for the effective performance of monitoring body's tasks.

26. As regards section 1.iii.C of the draft requirements, the use of sub-contractors implies that they will provide same guarantees and safeguards as the monitoring body. In this context, safeguards provided by sub-contractors cannot be proportionate but need to be the same as implemented by the monitoring body. Therefore, the Board recommend to delete a reference to "full proportion" in this section.

    As regards the same section, the Board would like to point out that a monitoring body is always responsible for the decision-making and for the compliance with the code. With respect to who should prepare the final decision, there is no doubt that it should be made by the monitoring body, not a sub-contractor, therefore the Board recommends to EL SA to use "shall" instead of "should" when referring to the monitoring body making the final decision. Lastly, the Board encourages EL SA to explicitly indicate that obligations applicable to the monitoring body are applicable in the same way to the sub-contractor.

    Finally, the Board is of the opinion that when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities. The Board encourages EL SA to introduce a direct reference to effective monitoring.

### 2.2.3 CONFLICT OF INTEREST

27. As regards section 2 of the draft accreditation requirements, the Board agrees with EL SA that the monitoring body shall have in place clear procedures to ensure that no natural or legal person carrying out code compliance monitoring tasks is linked, directly or indirectly, to the code member under scrutiny in such a way which may yield a conflict of interest. At the same time, the Board is of the opinion that such links should also be prohibited not only for code member, but also for the code owner and encourages EL SA to add the relevant reference.

    With respect to the same section, the Board underlines that monitoring body's personnel shall be obliged to report any situation likely to create a conflict of interest. A clear indication that personnel does not have any situation which could compromise its impartiality in decision making could be of use. In this context, the Board encourages the EL SA to add examples which would clarify in a better way what situation could likely constitute a conflict of interest.

### 2.2.4 EXPERTISE

28. As regards section 3 of the draft requirements, the Board is of the opinion that the monitoring body not "should", but, as it is obligatory, "shall" provide to the HDPA evidence that it has the expertise to undertake effective monitoring of a code. Also, the Board recommends to clarify what constitutes relevant qualifications (i.e. an in depth understanding and experience in relation to the specific data processing activities, appropriate data protection expertise and operational expertise) and to add a reference to relevant training, as an example.

29. The Board agrees with the EL SA, that expertise needs to involve the subject-matter (sector) of the code, in which case the relevant requirements that must be fulfilled can be specific, based on the sector to which the code applies. In this context, the Board recommends to clarify in section 3 that different interests involved and the risks of the processing activities addressed by the code should also be taken into account.

### 2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

30. With respect to section 4, the Board notes that it is mainly focussed on audits, however other ways to monitor controllers' and processors' compliance with the code should be included as well, for example review procedures, which can include such things as: audits, inspections, reporting and the use of self-monitoring reports or questionnaires. Also, the monitoring body shall demonstrate that it has a procedure for the investigation, identification and management of code member infringements to the code and additional controls to ensure appropriate action is taken to remedy such infringements as set out in the relevant code. In this context, the Board recommends to EL SA expanding this section to cover the above mentioned procedures.

    As regards the same section, the Board underlines that the issue of the procedures to check for eligibility of members prior to joining the code is also of importance. 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. Therefore, the Board recommends EL SA to reflect this in the text.

31. The Board recommends to EL SA to provide more information about what is approved policy and who approves it or when referring to "policy" in section 4, to delete the reference to "approved".

### 2.2.6 TRANSPARENT COMPLAINT HANDLING

32. In order to provide for more clarity, as regards section 5.A.b of the draft requirements, the Board recommends replacing the sentence "[i]n the event that the body finds the complaint vague or unsubstantiated, this shall be substantiated" with "[t]he monitoring body shall contact the complainant in order to give the complainant the opportunity to further substantiate the complaint/fill in the missing information".

33. With respect to section 5.A.e of the draft requirements, the Board, taking into account the importance of providing high level of transparency, recommends to EL SA to move the footnote to the main text.

34. In section 5.B.a of the draft requirements the Board encourages EL SA, for the sake of consistency, to replace the term “the person who submitted the complaint“ with “complainant”.

35. With respect to section 6.b of the draft requirements, the Board encourages EL SA to specify who assess what constitutes a relevant evidence. Also, the Board encourages EL SA to specify that such evidence includes information outlining details of the infringement and actions taken.

36. As regards section 6.d of the draft requirements, for the sake of consistency, the Board recommends to replace the wording “significant change has occurred to the monitoring body” with “substantial changes in relation to the structure and functioning of the monitoring body have occurred”.

### 2.2.7 REVIEW MECHANISMS

37. As regards section 7, 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 recommends EL SA to reflect this in the text.

### 2.2.8 LEGAL STATUS

38. The Board would like to underline that accreditation of a monitoring body does not extend to an assessment of compliance with the Regulation. Therefore, in section 8 of the draft requirements, the Board encourages EL SA to clarify what does “presumption of recognition” mean.

## 3 CONCLUSIONS / RECOMMENDATIONS

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

40. Regarding *general remarks* the Board recommends that the EL SA:

1. Replace in the second paragraph of the draft requirements the phrase “ensure compliance” with “help ensuring compliance” or “assist organisations in demonstrating compliance”.

2. In paragraph 10 of the draft requirements, remove a reference to the code owner, when mentioning request for renewal.

3. In paragraph 11 of the draft requirements, delete the last part of the last sentence, i.e. “which will be considered in separate guidelines”.

41. Regarding *independence* the Board recommends that the EL SA:

1. Elaborate and better explain in section 1 of the draft requirements what is the ability of a monitoring body to act independently.

2. In section 1.i.B of the draft requirements delete the word “current”.

3. In section 1.i.C of the draft requirements, add provision that an internal monitoring body cannot be setup within a code member.

4. In section 1.ii.A of the draft requirements, clarify that long-term financing should be ensured.

5. In section 1.iii.C of the draft requirements, delete a reference to "full proportion".

6. In section 1.iii.C of the draft requirements, use "shall" instead of "should" when referring to the monitoring body making the final decision.

42. Regarding *expertise* the Board recommends that the EL SA:

1. As regards section 3 of the draft requirements, clarify what constitutes relevant qualifications and that different interests involved and the risks of the processing activities addressed by the code should also be taken into account.

43. Regarding *established procedures and structures* the Board recommends that the EL SA:

1. With respect to section 4 of the draft requirements, expand it to cover different ways to monitor controllers' and processors' compliance with the code and to ensure appropriate action is taken to remedy possible infringements.

2. As regards the same section, add reference to procedures to check for eligibility of members prior to joining the code and provide more information about what is approved policy and who approves it.

44. Regarding *transparent complaint handling* the Board recommends that the EL SA:

1. As regards section 5.A.b of the draft requirements, replace the sentence "[i]n the event that the body finds the complaint vague or unsubstantiated, this shall be substantiated" with "[t]he monitoring body shall contact the complainant in order to give the complainant the opportunity to further substantiate the complaint/fill in the missing information".

2. With respect to section 5.A.e of the draft requirements, move the footnote to the main text.

3. As regards section 6.d of the draft requirements, for the sake of consistency, replace the wording "significant change has occurred to the monitoring body" with "substantial changes in relation to the structure and functioning of the monitoring body have occurred".

45. Regarding *review mechanisms* the Board recommends that the EL SA:

1. As regards section 7 of the draft requirements, make a direct indication that the monitoring body should 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.

# 4 FINAL REMARKS

46. This opinion is addressed to the Hellenic Supervisory Authority and will be made public pursuant to Article 64 (5) (b) GDPR.

47. According to Article 64 (7) and (8) GDPR, the EL 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.

48. The EL 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)