Opinion 1/2020 on the Spanish data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 28 January 2020

Adopted

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, as last modified and adopted on 10 September 2019

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 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, to provide written guidance explaining the accreditation requirements; and, finally, requesting them to adopt these 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 demonstrate how

[1] References to the "Union" made throughout this opinion should be understood as references to "EEA".

their proposed monitoring body meets the requirements set out in article 41 (2) 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 Spanish Supervisory Authority (hereinafter "ES 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 25 October 2019.

2. In compliance with article 10 (2) of the Board Rules of Procedure,[2] due to the complexity of the matter at hand, the Board 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

[2] Version 3, as last modified and adopted on 10 September 2019.

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 ES SA to take further action.

8. This opinion does not reflect upon items submitted by the ES 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 ES 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 wording in the ES SA's accreditation requirements is not in line with the terminology used in the Guidelines. For the sake of consistency and clarity, the EDPB encourages the ES SA to use the Guidelines terminology in the draft accreditation requirements. Examples include: "Accreditation requirements' instead of "Accreditation criteria" in the title, "code owners" instead of "code sponsor or code promoter", "code members" instead of "supervised bodies", "monitoring body" instead of

"supervisory body", "internal body" instead of "inside body", "establishment [of the monitoring body]" instead of "seat [of the monitoring body]". The paragraphs concerned are 1, 1.1, 1.2, 1.3, 1.4, 2, 3, 3.1, 3.2, 5.2, 5.3, 6.2, 6.3, 7.1, 8, and 8.2.

11. Whereas the Board acknowledges that reference to "should" might be due to the translation of the Spanish terms used to express obligation, the Board recommends that the ES SA amends the wording throughout the draft accreditation requirements, and replaces it with either "shall" or "must" in order to ensure the enforceability of the requirements.

12. The Board notes that there is no reference to the duration of the accreditation or accreditation withdrawal procedures. Whilst the Board accepts that these areas fall into the area of guidance supporting the accreditation requirements, the Board considers them to be important areas in terms of ensuring that the whole accreditation process is transparent. Therefore, the Board encourages the ES SA to clarify accreditation duration and withdrawal procedures in supporting guidance for the accreditation requirements.

13. Finally, the Board understands that, unless explicitly stated otherwise, the ES SA draft accreditation requirements apply to both internal and external monitoring bodies.

2.2.2 INDEPENDENCE

14. With regard to the introduction of section 1 of the draft accreditation requirements, the Board takes note of all the elements demonstrating the monitoring body's independency and impartiality of function in relation to the code members and the profession, industry or sector to which the code applies. However, there seems to be a contradiction between the third and fourth paragraphs of this section. In the third paragraph it is stated that the monitoring body should not have "*any dependency of any kind (organisational, economic, professional or personal) on the affiliated entity*", which seems to exclude the possibility of accrediting internal monitoring bodies on the basis of the fulfillment of this requirements. At the same time, in the last paragraph, there is mention of cases where the monitoring body is internal. Therefore, the Board recommends to the ES SA to clarify the relationship between these two paragraphs, and explain how independence can be achieved by an internal monitoring body, as well as to redraft the third paragraph so that internal monitoring bodies are suitably covered.

15. With regard to requirement 1.1, third bullet point, the Board considers that the wording "[...] *are being supervised* [...] *by the sponsor of the code of conduct, when the monitoring body is an inside body*" seems to weaken the separation between the code owners and the code members on the one hand, and the monitoring body on the other. Indeed, according to the Guidelines (paragraph 65, page 22), where an internal monitoring body is proposed, there should be separate staff and management, accountability and function from other areas of the code owners' organisation. In addition, the monitoring body, even if it is an internal one, should ensure adequate impartiality and independence on the basis of a risk management approach. Consequently, the Board recommends that the ES SA deletes the sentence "*or by the sponsor of the code of conduct, when the monitoring body is an inside body*", or otherwise clarify it, in line with the Guidelines.

16. As for the financial requirements (section 1.3 of the ES SA draft accreditation requirements), the Board acknowledges that monitoring bodies should be provided with the financial stability and resources

necessary for the effective performance of their tasks. The means by which a monitoring body receives financial support should not adversely affect the independence of its task of monitoring compliance of a code. The funding of the monitoring body and the transparency of such funding constitute a decisive element to assess the independence of the monitoring body. For this reason, the Board recommends that the ES SA deletes the phrase "where appropriate" and replaces "should" by "must be" or "have to be provided" in section 1.3 of the ES SA draft accreditation requirements.

17. Furthermore, section 1.4 of the ES SA draft accreditation requirements expressly refers to the "*cases where the monitoring body is an inside body [internal body]"*. The Board encourages the ES SA to clarify that the means of financing would not adversely affect the independence of the internal monitoring body.

18. The Board notes the requirement for the monitoring body to provide a description of resources available to it, in order to meet its liabilities as a result of its failure to perform its tasks (section 8.3 of the ES SA draft accreditation requirements). However, the Board is of the opinion that such a requirement might appear disproportionately burdensome for small and medium entities that might be discouraged from applying for accreditation. In this regard, the Board recommends that the ES SA softens the wording of this section, referring to the monitoring body's responsibilities in a general manner.

19. Regarding the publication of the monitoring body's report of annual activities (section 6.1), the Board recommends that, for the sake of clarity, the ES SA specifies the information that is deemed relevant for publication, as well as the level of detail of information that needs to be included in such reports.

20. The Board observes that there are no references to accountability as one of four areas in which the monitoring body shall demonstrate independence. According to the AT Opinion "*the monitoring body shall be able to demonstrate "accountability" for its decisions and actions in order to be considered to be independen*t" (Opinion on AT MB, paragraph 24). In this regard, the Board recommends that the ES SA includes the obligation to demonstrate independence in relation to the accountability of the monitoring body. For example, the ES SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. This could be accomplished through such things as setting out the roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the staff about the governance structures and the procedures in place.

2.2.3 CONFLICT OF INTEREST

21. The Board takes note of all the requirements included in the ES SA accreditation requirements in order for the monitoring body to demonstrate that the exercise of its tasks and duties does not result in a conflict of interest. However, the introduction under section 2 does not provide enough clarity as to which situations may result in a conflict of interest. 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 ES SA to add some examples, similar to the one provided in this paragraph.

2.2.4 EXPERTISE

22. Section 3 of the ES SA accreditation requirements refers to the "*promoters of the code of conduct*" and "sponsor of the code" (understood as code owners) and the monitoring body, who need to demonstrate that "*the persons in charge of taking decisions have the necessary knowledge in relation to data protection legislation and practice* [...]*"*. The Board is of the opinion that reference to the obligation of the code owners to demonstrate the expertise of the monitoring body could be misleading. Indeed, it might be appropriate in case of an internal monitoring body applying for accreditation, whereas in the case of an external monitoring body, it would be the body itself, applying for accreditation, that would need to demonstrate its expertise. Therefore, the Board encourages the ES SA to delete the phrases "*promoters of the code of conduct*" and "*sponsor of the code*" in order to refer to both internal and external monitoring bodies.

23. Furthermore, the Board encourages the ES SA to align the first paragraph of this section to the Guidelines, by including reference to the required expertise in "[...] *data protection legislation and practice in the* processing activities *of the sector* [...]". Finally, the Board encourages the ES SA to clarify the third paragraph of this section by indicating that the requirement for expertise applies to the monitoring body as a whole and not to every staff member.

24. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (in section 6.4 of the Guidelines), by demonstrating "*why their proposals for monitoring are appropriate and operationally feasible*" (paragraph 41, page 17 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code's monitoring activities effectively. Section 3.1 of the ES SA draft accreditation requirements refers to the "*means to demonstrate the necessary skill, knowledge and experience*". A reference to the level of experience as required by the code itself is missing. The Board encourages the ES SA to add examples so that the data protection expertise, experience and knowledge required, are reflected in the Code itself.

25. Section 3.2 of the ES SA draft accreditation requirements provides only a general description of the expertise requirements. The Board encourages the ES SA to provide a detailed description of the expertise requirements and clarify whether the requirements set in paragraph 69 of the Guidelines are covered.

26. Finally, in order for these requirements to be actual requirements, rather than guidance, the Board encourages the ES SA redraft all three requirements to start with "*the monitoring body shall…*".

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

27. The Board notes that requirement 5.2 of the ES SA accreditation requirements states that the complaint handling procedure will be transparent and easily accessible to the public. The Board acknowledges that this wording is based on the Guidelines. Nonetheless, the Board is of the opinion that, for the sake of clarity, the requirements should specify the meaning of "public" and whether it also includes code members. Therefore, the Board encourages the ES SA to amend requirement 5.2 accordingly.

28. The Board observes that among the factors to consider when assessing the details of the procedures aiming at monitoring the compliance of the code members with the code of conduct (section 4.1,

second bullet point of the ES SA draft accreditation requirements) the requirement refers to "*the number of members*". It is unclear, how the assessment of the ES SA could be based on this criterion, considering that the numbers of the code members might not be known when the monitoring body applies for accreditation and might change considerably after the accreditation has been granted. Among the said factors, there is also a reference to "*the number of complaints received*". Whereas the number of complaints could be relevant, the focus thereof is probably more relevant as a criterion, but it is not included. Furthermore, the Board considers that other elements, such as the focus of the complaints, might have a greater significance. In this regard, the Board encourages the ES SA to replace the term "*the number of members*" with "*expected number and size of members*" and to delete reference to the "*number*" of complaints, and keep it more general, such as "*the received complaints*".

2.2.6 TRANSPARENT COMPLAINT HANDLING

29. Regarding the complaints about code members (section 5.2 of the ES SA draft accreditation requirements), the Board acknowledges that the complaints handling process requirements should be set at a high level and reference reasonable time frames for answering complaints. In this regard, the Board notes that the ES SA draft accreditation requirements state that the complaints procedure should be resolved "*within a reasonable period of time not exceeding three (3) months*". In the event that, by the term "*resolve*", the ES SA refers to the final decision of the investigation, the Board recommends the ES SA to take a more flexible approach, by stating that the monitoring body will have to provide the complainant with progress reports or the outcome within a reasonable timeframe, such as three months. If the ES SA refers to another kind of resolve, different from the final decision of the investigation, the Board recommends the ES SA to clarify what kind of information it is referring to.

30. Furthermore, the Board takes note of the fact that the three months deadline could be extended where necessary, considering the size of the company under investigation, as well as the difficulty of the investigation.

31. The Board observes that section 5.2, fifth bullet point of the ES SA draft accreditation requirements only refers to "*penalties*". In the Board's opinion, this requirement seems to restrict the margin of manoeuver of the monitoring body with regard to the kind of measures it can apply. In addition, those measures must be determined in the code of conduct, as per article 40(4) GDPR. The Board considers that a more comprehensive wording would include reference to remedies and corrective measures and encourages the ES SA to replace "*penalties*" with "*sanctions*". Those corrective measures must be determined in the code of conduct, as per article 40(4) GDPR. Therefore, for the sake of clarity, the Board recommends the ES SA to add a reference to the list of sanctions set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.

32. The Board observes that the ES SA decides, for the purpose of transparency of the complaints handling procedure, to require that the monitoring body publishes the decisions taken in the context of the complaint handling procedure (section 5.2). Publication of final decisions could have the same effect of an accessory sanction for the code member to which the decision is addressed. However, the Board acknowledges that general information on the actions taken by the monitoring body in case of infringement of the code of conduct would enhance transparency. Thus, for the sake of clarity, the Board recommends that the ES SA specifies the kind of relevant information that the monitoring body

is obliged to publish. For example, the monitoring body could publish, on a regular basis, statistical data with the result of the monitoring activities, such as the number of complaints received, the type of infringements and the corrective measures issued.

2.2.7 COMMUNICATING WITH THE AEPD

33. The Board observes that there is no reference to a deadline by which the monitoring body should inform the AEPD in the event of a substantial change (section 6.2 of the ES SA draft accreditation requirements). Therefore, the Board recommends that the ES SA rephrases the requirement to cover appropriate time expectations for the communication to the AEPD. For example, a substantial change shall be communicated to the ES SA "without undue delay". Furthermore, the "*scope of accreditation*" is amongst the substantial changes that shall be reported to the SA (section 6.2, fourth bullet point). The Board considers this inclusion misleading, since the monitoring body cannot change the scope of the accreditation. Therefore, the Board recommends that the ES SA deletes reference to the scope of accreditation or, alternatively, clarify the meaning thereof.

34. The Board observes that section 6.3 of the ES SA accreditation requirements refers to the elements that communication to the AEPD should contain; the reasons for the decision as well as the criteria on which the suspension is based. For reasons of clarity, the Board recommends that reference to "exclusion" is added as well.

2.2.8 CODE REVIEW MECHANISMS

35. The Board considers that the requirements under section 7.1 appear to be too strict and might lead to excessive standards for the monitoring body, especially the third and fourth bullet points. It should be sufficient that the monitoring body shall inform the code owner and recommend that the relevant parts of the code are revised in accordance with the evaluation. In addition, this requirement should envisage the possibility that the information listed in it is not provided to the code owner, but to any other entity referred to in the code of conduct, in order to give some margin of manoeuvre to the code owners in designing the procedure for assessing the necessity of a revision of the code. In this regard, the Board encourages the ES SA to rephrase the last two bullet points, so that they appear less restrictive, as well as include information to remedy the identified shortcomings. Furthermore, the Board considers that more flexibility should be allowed, and encourages the ES SA to take into consideration that the information listed in the requirement may be not be provided to either the code owner, or to any other entity referred to in the code of conduct and add the above-mentioned reference.

2.2.9 LEGAL STATUS

36. Section 8.1 of the ES SA draft accreditation requirements includes reference to the legal personality of the monitoring body; however, an internal monitoring body is unlikely to have a legal personality. This requirement would in fact impede an internal monitoring body from applying for accreditation.

Consequently, the Board recommends to the ES SA to delete reference to the "*legal personality*" in order to clarify that internal monitoring bodies are not excluded.

37. Finally, the Board notes that the ES SA's requirements or explanatory notes do not reference subcontracting, leaving this area open for monitoring bodies applying for accreditation to decide upon. The Board recommends that ES SA clarifies whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the explanatory notes or ordinance accordingly. If ES SA indicates that subcontracting is allowed, the Board recommends that the ES SA indicates, in the requirements, that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

3 CONCLUSIONS / RECOMMENDATIONS

38. The draft accreditation requirements of the Spanish 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 ES SA:

1. replaces "*should*" with "*shall*" or "*must*" throughout the text, in order to ensure the enforceability of the requirements.

40. Regarding *independence* the Board recommends that the ES SA:

1. clarifies and explains how independence can be achieved by an internal monitoring body in section 1;

2. deletes the following sentence "*or by the sponsor of the code of conduct, when the monitoring body is an inside body*" from requirement 1.1, third bullet point, or otherwise clarify it, so that the requirements of independence and impartiality, as set in the Guidelines, are met;

3. adjusts the wording in requirement 1.3, in order to ensure that the funding of the monitoring body does not affect its independency;

4. softens the wording of requirement 8.3, referring to the monitoring body's responsibilities in a general manner so that this requirement appear less burdensome for small and medium entities applying for accreditation;

5. specifies which information of the monitoring body's report on annual activities is deemed relevant for publication, as well as the level of detail of information that needs to be included in such reports;

6. includes the obligation to demonstrate independence in relation to the accountability of the monitoring body. Regarding *transparent complaint handling* the Board recommends that the ES SA:

1. adopts a more flexible approach in requirement 5.2, regarding the timeline for resolving complaints;

2. includes reference to remedies and corrective measures in requirement 5.2;

3. specifies the kind of relevant information that the monitoring body is obliged to publish with regards to the final decisions adopted.

41. Regarding *communication with the AEPD* the Board recommends that the ES SA:

1. rephrases requirement 6.2 in order to cover appropriate time expectations for the communication to the AEPD;

2. deletes reference to the scope of accreditation or, alternatively, clarify the meaning thereof in requirement 6.2, fourth bullet point;

3. adds reference to "exclusion" in requirement 6.3, for reasons of clarity.

42. Regarding *legal status* the Board recommends that the ES SA:

1. deletes reference to the "*legal personality*" in requirement 8.1 in order to clarify that internal monitoring bodies are not excluded;

2. clarifies whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the requirements or explanatory notes. If subcontracting is allowed, amend the requirements or explanatory notes, so that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

4 FINAL REMARKS

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

44. According to Article 64 (7) and (8) GDPR, the supervisory authority 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. The supervisory authority 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)